Laís Ramos Pereira da Silva

Do Algoritmo RSA à Sala de Aula: A Criptografia como Ferramenta de Ensino

Vitória

2025

Laís Ramos Pereira da Silva

Do Algoritmo RSA à Sala de Aula: A Criptografia como Ferramenta de Ensino

Dissertação de mestrado apresentada ao PROFMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Orientador: Prof. Dr. Alcebíades Dal Col Júnior

Vitória

2025

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Silva, Laís Ramos Pereira da, 1996-
S586a Do algoritmo RSA à sala de aula: A criptografia como ferramenta de ensino / Laís Ramos Pereira da Silva. - 2025.
88 f. : il.

Orientador: Alcebiades Dal Col Júnior.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Computação - Matemática. 2. Matemática. 3. Criptografia. 4. Números primos. I. Dal Col Júnior, Alcebiades. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT

“Do Algoritmo RSA à Sala de Aula: A Criptografia como Ferramenta de Ensino”

Laís Ramos Pereira da Silva

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 25/04/2025 por:

_____

Prof.(a) Dr.(a) Alcebíades Dal Col Júnior
Orientador(a) – UFES

_____

Prof.(a) Dr.(a) Moacir Rosado Filho
Membro Interno – UFES

_____

Prof.(a) Dr.(a) Fidelis Zanetti de Castro
Membro Externo – IFES

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 30/04/2025 às 20:15:53

Folha de Assinaturas Laís Ramos Pereira da Silva

Data e Hora de Criação: 25/04/2025 às 10:30:02

Documentos que originaram esse envelope:
- Folha de Assinaturas Laís Ramos Pereira da Silva.pdf (Arquivo PDF) - 1 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: e330493c85b4dfba528974d1833057916f99493fefff27e5c592d746752e6f98
[SHA512]: c88d62a6976ffb8d187bb96b14576c352c4bb9f0691532bba6abace30ce3fd2fca0df978bfb9fffa17c086ca470ee3d1548b286c0f1f770230be7f10be186354

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Alcebiades Dal Col Júnior (alcebiades.col@ufes.br)
Data/Hora: 28/04/2025 - 07:59:42, IP: 189.48.54.30, Geolocalização: [-20.345651, -40.38656]
[SHA256]: f92e1bb1898a03476a1fdb62b4ef9e2ee1069ea418213b9c4bb275cbac60d936

ASSINADO - Moacir Rosado Filho (moacir.rosado@ufes.br)
Data/Hora: 30/04/2025 - 00:04:27, IP: 179.95.220.104, Geolocalização: [-20.295008, -40.296595]
[SHA256]: 377c1ce13ca20e734ef5aaf667b858624f618b46bfc96880046689cd75718d68

ASSINADO - Fidelis Zanetti de Castro (fidelis.castro@gmail.com)
Data/Hora: 30/04/2025 - 20:15:53, IP: 191.248.34.66, Geolocalização: [-20.191641, -40.248934]
[SHA256]: dc53bb9473e5c2c1cabd96fb76444799387388962d95adcce9a5aabb8a97363e

Histórico de eventos registrados neste envelope

30/04/2025 20:15:53 - Envelope finalizado por fidelis.castro@gmail.com, IP 191.248.34.66
30/04/2025 20:15:53 - Assinatura realizada por fidelis.castro@gmail.com, IP 191.248.34.66
30/04/2025 20:15:43 - Envelope visualizado por fidelis.castro@gmail.com, IP 191.248.34.66
30/04/2025 00:04:27 - Assinatura realizada por moacir.rosado@ufes.br, IP 179.95.220.104
28/04/2025 07:59:42 - Assinatura realizada por alcebiades.col@ufes.br, IP 189.48.54.30
28/04/2025 07:59:06 - Envelope visualizado por alcebiades.col@ufes.br, IP 189.48.54.30
25/04/2025 10:30:13 - Envelope registrado na Blockchain por ivan.barbosa@ufes.br, IP 189.48.23.154
25/04/2025 10:30:12 - Envelope encaminhado para assinaturas por ivan.barbosa@ufes.br, IP 189.48.23.154
25/04/2025 10:30:03 - Envelope criado por ivan.barbosa@ufes.br, IP 189.48.23.154

Toda honra e toda glória deste trabalho pertencem a Deus.

Agradecimentos

A Deus, por me guiar em todos os momentos e me dar força para superar os desafios desta caminhada.

Ao meu pai e à minha mãe, Luís David e Marinete, pelo amor incondicional, pelo apoio e por sempre acreditarem em mim. Sem vocês, nada disso seria possível.

À minha madrinha Kelly e ao meu padrinho Marcos, por todo carinho, motivação e apoio inestimável.

Às minhas amigas de sala, Débora e Gabriela, por compartilhar comigo essa jornada acadêmica, pelos incentivos, pelas conversas e pelo companheirismo ao longo do curso.

Aos meus amigos Nayara e Júnior, pela amizade, pelas palavras de incentivo e por estarem sempre presentes ao longo dessa trajetória.

À minha família, de maneira geral, por sempre estarem ao meu lado, me encorajando e celebrando cada conquista comigo.

Aos professores Dr. Alcebíades, Dr. Florêncio, Dr. Valmecir, Dr. Moacir e Dra. Rosa Elvira, pela orientação, ensinamentos e apoio durante essa trajetória acadêmica.

Aos meus alunos e alunas do 6ºF (2023) e 7º F (2024) da UMEIEF Professora Flávia Borgo que acompanharam esse momento da minha vida acadêmica e foram essenciais para a minha paixão e crença pela educação pública de qualidade.

Resumo

A criptografia RSA é baseada na dificuldade de decompor números compostos grandes em fatores primos. Sendo um tema relevante para o Ensino Médio, sua aplicação prática se conecta a conceitos fundamentais da matemática. Seu estudo explora tópicos como números primos, divisão euclidiana e propriedades de potência e desta forma, é promovido um aprendizado interdisciplinar entre a matemática e a computação. Em sala de aula, a abertura do assunto pode ser introduzida com a evolução histórica do assunto, de forma acessível elaborar exemplos simplificados que mostram a geração de chaves públicas e privadas, para o processo de codificação e decodificação de mensagens e simular troca de informações seguras entre alunos, para que eles possam compreender a importância da aritmética na proteção de dados no computador. Além disso, os componentes curriculares abordados estimulam o pensamento crítico, a resolução de problemas, entre outros assuntos.

Palavras-chave: Criptografia RSA, codificação, decodificação, chave pública, chave privada, números primos, congruência modular, divisão euclidiana.

Abstract

RSA cryptography is based on the difficulty of factoring large composite numbers into prime factors. As a relevant topic for high school education, its practical application connects to fundamental mathematical concepts. Its study explores topics such as prime numbers, the Euclidean division, and properties of exponentiation, thus promoting an interdisciplinary learning experience between mathematics and computer science. In the classroom, the topic can be introduced through its historical evolution, followed by accessible and simplified examples that demonstrate the generation of public and private keys, the process of encoding and decoding messages, and the simulation of secure information exchange among students. This approach helps them understand the importance of arithmetic in protecting computer data. Additionally, the curricular components covered stimulate critical thinking, problem-solving, and other related topics.

Keywords: RSA cryptography, encoding, decoding, public key, private key, prime numbers, modular congruence, Euclidean division.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

Qual professor de matemática, seja do Ensino Básico ou Ensino Superior, nunca ouviu a seguinte pergunta: “Mas professor(a), para que isso serve?” Ou a afirmação: “Isso não serve para nada”. E na maioria das vezes, os licenciados na disciplina de Matemática, não se preocupam com a aplicação do conteúdo na vida do aluno. A verdade é que a matemática está inserida em muitas áreas da vida de qualquer pessoa.

Pensando em apresentar a Matemática de maneira mais atrativa, foi de interesse buscar um tema com relevância histórica para divulgação Científica. Por isso, será iniciada uma pesquisa sobre a história da criptografia e irá se desenvolver ao londo do trabalho o estudo sobre a álgebra e a aritmética por trás do assunto.

Com a motivação de ensinar sobre criptografia, no Capítulo 2, o objetivo será abordar os conhecimentos sobre a história da criptografia. Conteúdo essencial para ser compreendido a necessidade de seu uso desde a antiguidade até a atualidade. Com seu principal referencial embasado nas obras de SINGH (SINGH, 2004), COSTA e FIGUEIREDO (COSTA C.; FIGUEIREDO, 2010), (FIARRESGA, 2010) e HEFEZ (HEFEZ, 2014) da própria coleção do PROFMAT, Aritmética.

No Capítulo 3, será estudado a fundamentação teórica para o conceito da criptografia RSA, com definições, teoremas e corolários para ser entendida a matemática por trás da criptografia RSA.

Em um mundo cada vez mais digital e conectado, a segurança da informação se tornou uma prioridade essencial para proteger dados pessoais, de comércio e de governos. A criptografia, método de transformar informações legíveis em códigos ilegíveis, surge como a principal ferramenta para garantir o sigilo, totalidade e veracidade dos dados. Desde as civilizações antigas, que usavam técnicas rudimentares para proteger as mensagens de espionagem, até os algoritmos avançados de hoje, a criptografia se desenvolveu de modo a responder às necessidades crescentes por segurança em um ambiente de constante mudança.

A criptografia moderna compreende um conjunto de assuntos matemáticos complexos, utilizados para embaralhar dados de tal forma que apenas pessoas ou sistemas autorizados possam decifrar os conteúdos. Na prática, essa tecnologia protege desde senhas e transações bancárias até diálogos importantes entre governos. De acordo com COUTINHO (COUTINHO., 2015), o objetivo principal da criptografia é impedir o acesso não autorizado a informações críticas, assegurando, ao mesmo tempo, que essas informações possam ser recuperadas de maneira íntegra por aqueles a quem elas se destinam. A importância da criptografia cresceu de forma extraordinária com o avanço da internet e

das comunicações digitais.

Um dos métodos mais utilizados para proteger informações frágeis é a criptografia RSA. Por este motivo, no Capítulo 4 será apresentado o algoritmo da criptografia. O RSA é um sistema que utiliza um par de chaves (uma pública e uma privada) para garantir a proteção dos dados. Desenvolvida por Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman em 1977, o **RSA** se baseia na dificuldade de decompor números muito grandes em fatores primos. A chave pública é usada para criptografar a mensagem, enquanto a chave privada, conhecida apenas pelo destinatário, permite a sua decodificação. Esse mecanismo assegura que, mesmo que a comunicação seja interceptada, o conteúdo permanece inacessível a terceiros, a menos que possuam a chave privada. Graças a essa metodologia, a criptografia RSA é amplamente utilizada nos tempos atuais, destacando de forma clara a aplicação prática da matemática na segurança digital.

No Capítulo 5, de acordo com a Base Nacional Comum Curricular (BRASIL. Ministério da Educação, 2018), será proposta uma sequência didática que visa melhorar as competências matemáticas e promover a compreensão dos estudantes ao aplicarem conceitos de aritmética e teoria dos números.

2 A história da Criptografia

A criptografia está presente em quase todos os aspectos do nosso dia a dia, como em transações bancárias, compras online e até em aplicativos de mensagens, como o WhatsApp, que é amplamente utilizado no Brasil. Mas, para entender melhor o papel da criptografia atualmente, é interessante fazer uma viagem ao passado e compreender como e por que ela começou a ser utilizada.

A palavra criptografia vem do grego, das palavras *kriptos* que significa escondido e *grapho* que significa escrita, ou seja, é um jeito de você embaralhar uma mensagem de uma forma que nenhum desconhecido, além de seu destinatário, consiga entender o que o remetente escreveu.

Neste capítulo, iremos explorar a história da criptografia, inspirada em algumas leituras que serão referenciadas ao longo do texto. Buscaremos entender quando essas técnicas foram usadas para enviar mensagens secretas e os resultados dessas ações. No mundo antigo, por exemplo, a criptografia era uma ferramenta essencial para confundir inimigos de guerra e garantir que as mensagens fossem transmitidas com segurança. Segundo FIARRESGA (FIARRESGA, 2010), os primeiros registros do uso dessa forma de comunicação foram encontrados no Egito, dentro da tumba de Khnumhotep II, por volta de 1900 anos antes de Cristo. No entanto, foi cerca dos anos 400 a.C., na Roma Antiga, que a criptografia ganhou destaque, especialmente com o uso da famosa cifra usada por Júlio César.

2.1 A Cifra de César

De acordo com SINGH (SINGH, 2004), uma de suas primeiras formas de uso de criptografia foi na Roma antiga. Por causa de longos períodos de guerra, o político e líder, Caio Júlio César, precisava enviar mensagens para os campos de batalha sem que nenhum inimigo que cruzasse o caminho do mensageiro descobrisse o real conteúdo do texto. Por isso, era empregue a chamada cifra de César que foi utilizada para o governo se comunicar com os generais romanos.

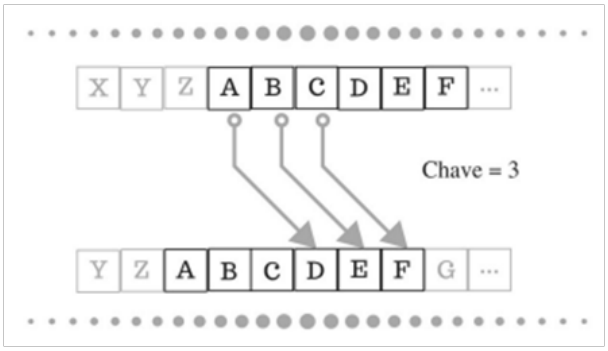
O sucesso das conquistas territoriais no governo de Júlio César pode ser explicado pelo esquema de segurança e por outros fatores que também foram decisivos. A habilidade de César como estrategista militar, o preparo das legiões romanas, as alianças que ele pôde construir foram cruciais para suas vitórias. Além disso, o sistema criptográfico foi um fator importante para o crescimento do império romano.

Figura 1 – O mapa mostra o território Romano, em amarelo.

Fonte: Disponível em:<https://historiasderoma.com/category/julio-cesar/>. Acesso em 26 de julho 2024.

A cifra de César é uma cifra de substituição, isso significa que cada letra do alfabeto é deslocada uma certa quantidade de vezes e então é substituída por outra letra. Esse número de vezes que o alfabeto é transposto é uma espécie de senha ou chave que o receptor precisa saber para iniciar o processo de decodificação da mensagem. A Figura 2 exemplifica a chave escolhida por César, 3.

Figura 2 – A Cifra de César.



Fonte: Disponível em: <https://www.clei.org/LAWCC/lawcc2018/lawcc2018-p15.pdf>. Acesso em 26 de julho 2024.

O alfabeto português é composto por 26 letras, então, para cada letra, existem 25 possibilidades de deslocamento (excluindo o deslocamento 0). Significando que para uma mensagem com X letras do alfabeto usado no Brasil, existem 25 chaves possíveis de serem usadas.

Exemplo 2.1.1. *César deseja enviar uma mensagem oculta para seu general em um campo de batalha usando a chave 3 de sua cifra que já é conhecida pelo seu militar.*

Mensagem original: "ATACAR AO AMANHECER"

Mensagem cifrada: "DWDGDU DR DPDPKHFHU"

De acordo com COSTA E FIGUEIREDO (COSTA C.; FIGUEIREDO, 2010), após 1000 anos de uso esse segredo foi descoberto pelos árabes. Com as mensagens interceptadas por eles, houve uma análise de frequência de letras nas palavras de acordo com o alfabeto usado. Para melhor entendimento, foi feita uma pesquisa, mostrada na Tabela 1, sobre o percentual de presença das letras nas palavras da Língua Portuguesa. Como observado no Exemplo 2.1.1, a letra "A" foi a que mais apareceu na frase, se tornando "D". Com isso, houve o reconhecimento de palavras comuns, como artigos e preposições por meio da substituição simples de letras.

Tabela 1 – Percentual de frequência das letras em palavras em Português.

Letra	**Frequência**	**Letra**	**Frequência**
A	14,64%	N	5,05%
B	1,04%	O	10,73%
C	3,88%	P	2,52%
D	4,1%	Q	1,2%
E	12,57%	R	6,53%
F	1,02%	S	7,81%
G	1,3%	T	4,34%
H	1,28%	U	4,64%
I	6,18%	V	1,7%
J	0,4%	W	0,01%
K	0,02%	X	0,21%
L	2,78%	Y	0,01%
M	4,75%	Z	0,47%

Fonte: (COUTINHO., 2015)

Com a descoberta do segredo de César, houve a necessidade de ser criado outro código, chamado cifra indecifrável de Vigenère.

2.2 Bastão de Licurgo

O bastão de Licurgo, conhecido também como citale espartano, é considerada a mais antiga cifra de transposição. Segundo SINGH (SINGH, 2004) , "uma cifra de transposição é aquela em que cada letra de uma mensagem altera sua posição no texto, mas mantém sua identidade". Essa técnica foi empregada por volta de 475 a.C., sendo considerada um dispositivo criptográfico utilizado em contextos militares.

O Bastão de Licurgo era uma fita que o remetente enrolava num bastão e lá escrevia a mensagem como no exemplo da Figura 3. Após a mensagem ter sido escrita, a fita virava

o cinto do encarregado de viajar com o recado até o recebedor. A pessoa que recebia a mensagem precisava dispor de um bastão de mesmo diâmetro usado pelo remetente.

O método de criptografia usado no bastão de Licurgo pode ser compreendida como um processo de reestruturação de letras em uma tabela, que chamamos na matemática de matriz. A mensagem é escrita ao redor do bastão, como se fosse organizada em várias linhas e colunas.

Exemplo 2.2.1. *Suponha que planejamos enviar a mensagem em inglês como na Figura 3: "KILL KING TOMORROW MIDNIGHT" ("MATE O REI AMANHÃ À MEIA-NOITE"), teremos a mensagem sem espaço entre as palavras, desta forma: "KILLKINGTOMORROWMIDNIGHT", composta por 24 caracteres. Vamos dividir o tamanho da mensagem, ou seja, 24 caracteres, pelo número de colunas. Adotemos como chave 8 colunas (comprimento do bastão). Desse modo, teremos 3 linhas, pois a divisão de 24 por 8 é igual a 3.*

Figura 3 – Bastão de Licurgo.

Fonte: (FIARRESGA, 2010)

Logo pela Figura 3, o texto codificado seria: "KTMIOILMDLONKRIIRGNOHGWT".

2.3 A cifra de Vigenère

Segundo SINGH (SINGH, 2004), Blaise de Vigenère foi um diplomata francês que ficou conhecido por sua contribuição à criptografia. Ele foi a grande estrela na criação da cifra que carrega seu nome, a Cifra de Vigenère.

Figura 4 – Blaise de Vigenère.

Fonte: Disponível em: <https://monbourbonnais.com/vigenere-de-blaise-ecrivain-diplomate/.>. Acesso em: 10 de agosto de 2024.

No começo ela foi baseada na própria cifra de César, e depois foi preenchida por uma matriz, com uma coluna que vai de "A" a "Z" e uma linha que também vai de "A" a "Z", ou seja, é uma matriz 26×26 e para criptografar, usamos a interseção da linha da letra da chave com a coluna da letra da mensagem.

Exemplo 2.3.1. *Como mostrado na Tabela 2, é possível criptografar mais uma vez, a frase "ATACAR AO AMANHECER" e com a chave "PROFMAT", tal qual no Exemplo 2.1.1:*

Tabela 2 – Matriz 26×26 usada na Cifra de Vigenère.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Produção da própria autora (2024).

Mensagem original: "ATACAR AO AMANHECER"

Chave: "PROFMAT"

Reprodução da chave em toda extensão da mensagem original:

"PROFMA TP ROFMATPRO"

Mensagem cifrada: PKOHMR TD RAFZHXRVF

É interessante reproduzir a codificação do Exemplo 2.3.1 em matemática, pelo fato de ser possível descrever a Cifra de Vigenère utilizando a congruência modular. Considerando que o leitor é familiarizado com alguns conceitos de aritmética, podemos representar as letras dos alfabeto em números, facilitando a análise para codificar e decodificar uma mensagem.

1. Transformar cada letra do alfabeto em número de acordo com a Tabela 3:

Tabela 3 – Tabela para transformação de letra em número.

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Valor	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Valor	13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Produção da própria autora.

2. Converter cada letra da mensagem original e da chave em números e somar os valores correspondentes da mensagem e da chave, como na tabela.

Tabela 4 – Transformação de letra em número.

Mensagem original	A	T	A	C	A	R	A	O	A	M	A	N	H	E	C	E	R
Valor	0	19	0	2	0	17	0	14	0	12	0	13	7	4	2	4	17
Chave	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R	O
Valor	15	17	14	5	12	0	19	15	17	14	5	12	0	19	15	17	14
Soma	15	36	14	7	12	17	19	29	17	26	5	25	7	23	17	21	31

Fonte: Produção da própria autora.

3. Converter os números resultantes de volta em letras usando congruência módulo 26:

Tabela 5 – Transformação de números em letras.

$15 \equiv 15 \pmod{26}$	$15 = \mathrm{P}$
$36 \equiv 10 \pmod{26}$	$10 = \mathrm{K}$
$14 \equiv 14 \pmod{26}$	$14 = \mathrm{O}$
$7 \equiv 7 \pmod{26}$	$7 = \mathrm{H}$
$12 \equiv 12 \pmod{26}$	$12 = \mathrm{M}$
$17 \equiv 17 \pmod{26}$	$17 = \mathrm{R}$
$19 \equiv 19 \pmod{26}$	$19 = \mathrm{T}$
$29 \equiv 3 \pmod{26}$	$3 = \mathrm{D}$
$17 \equiv 17 \pmod{26}$	$17 = \mathrm{R}$
$26 \equiv 0 \pmod{26}$	$0 = \mathrm{A}$
$5 \equiv 5 \pmod{26}$	$5 = \mathrm{F}$
$25 \equiv 25 \pmod{26}$	$25 = \mathrm{Z}$
$7 \equiv 7 \pmod{26}$	$7 = \mathrm{H}$
$23 \equiv 23 \pmod{26}$	$23 = \mathrm{X}$
$17 \equiv 17 \pmod{26}$	$17 = \mathrm{R}$
$21 \equiv 21 \pmod{26}$	$21 = \mathrm{V}$
$31 \equiv 5 \pmod{26}$	$5 = \mathrm{F}$

Fonte: Produção da própria autora.

A frase “ATACAR AO AMANHECER” cifrada com a chave “PROFMAT” fica: “PKOHMR TD RAFZHXRVF”.

Por dedução, a fórmula para cifragem da Cifra de Vigenère usando congruência modular:

P_i = o valor numérico da i-ésima letra do texto original;

K_i = o valor numérico da i-ésima letra da chave;

C_i = o valor numérico da i-ésima letra do texto cifrado, onde $C_i = P_i + K_i$.

$$\begin{cases} C_i \equiv C_i \pmod{26}, & \text{se } 0 \leq C_i < 26; \\ C_i \equiv C_i - 26 \pmod{26}, & \text{se } 26 \leq C_i < 51 \end{cases} \tag{2.1}$$

Agora, para fazer o caminho inverso e decifrar a frase "PKOHMR TD RAFZHXRVF" usando a chave "PROFMAT" e empregando a cifra de Vigenère, será preciso subtrair a posição da letra da chave da posição da letra cifrada e converter o resultado em letras para obter o texto original, como pode ser visualizado na Tabela 6.

Tabela 6 – Descriptografia de Vigenère.

Letra cifrada	**Letra da chave**	**Subtração**	**Letra decifrada**
P = 15	P = 15	$15 - 15 = 0$	0 = A
K = 10	R = 17	$10 - 17 = -7 \equiv 19 \pmod{26}$	19 = T
O = 14	O = 14	$14 - 14 = 0$	0 = A
H = 7	F = 5	7 - 5 = 2	2 = C
M = 12	M = 12	12 - 12 = 0	0 = A
R = 17	A = 0	17 - 0 = 17	17 = R
T = 19	T = 19	19 - 19 = 0	0 = A
D = 3	P = 15	$3 - 15 = -12 \equiv 14 \pmod{26}$	14 = O
R = 17	R = 17	$17 - 17 = 0$	0 = A
A = 0	O = 14	$0 - 14 = -14 \equiv 12 \pmod{26}$	12 = M
F = 5	F = 5	5 - 5 = 0	0 = A
Z = 25	M = 12	25 - 12 = 13	13 = N
H = 7	A = 0	7 - 0 = 7	7 = H
X = 23	T = 19	23 - 19 = 4	4 = E
R = 17	P = 15	17 - 15 = 2	2 = C
V = 21	R = 17	21 - 17 = 4	4 = E
F = 5	O = 14	$5 - 14 = -9 \equiv 17 \pmod{26}$	17 = R

Fonte: Produção da própria autora.

Mensagem Decifrada: ATACAR AO AMANHECER

Por dedução, a fórmula para decodificar a Cifra de Vigenère usando congruência modular:

C_i =o valor numérico da i-ésima letra do texto cifrado;

K_i = o valor numérico da i-ésima letra da chave;

P_i = o valor numérico da i-ésima letra do texto original, onde $P_i = C_i - K_i$.

$$\begin{cases} P_i \equiv P_i \pmod{26}, & \text{se } 0 \leq P_i < 26; \\ P_i \equiv P_i + 26 \pmod{26}, & \text{se } -26 < P_i < 0 \end{cases} \tag{2.2}$$

A Cifra de Vigenère é um esquema criptográfico, muito mais seguro que o de substituição simples, devido à extensão de sua chave. Entretanto, a complexidade em seu algoritmo, dificulta sua aplicação, deixando com que seu uso não detivesse boa aceitação. Com o passar dos anos a Cifra de Vigenère foi descoberta e métodos de criptografia mais avançados foram desenvolvidos, como a máquina enigma.

2.4 Criptografia na 2ª Guerra Mundial

A 2ª Guerra Mundial foi um dos conflitos mais extremos dos últimos tempos, com duração de 1938 a 1945 e causou milhões de mortes. Sendo, de um lado a Alemanha e os demais países do Eixo, do outro, os países Aliados juntamente com a Inglaterra, que possuía o melhor serviço de inteligência militar e por causa desse sistema dos ingleses, centenas de embarcações carregando materiais para Europa foram salvos de serem afundados por submarinos. Além da vantagem tática de saber a comunicação inimiga em tempo real nos três últimos anos da guerra.

Em 1918, antes do início da 2ª Guerra Mundial, foi inventada pelos alemães uma máquina chamada "Enigma". Criada originalmente com o objetivo de proteger comunicações comerciais, com sua aparência similar a uma máquina de escrever, mas com sistema chamado de máquinas de rotor, especificamente 3 rotores, e, segundo TKOTZ (TKOTZ, 2005), a codificação de suas mensagens tinham 105.869.167.644.240.000 de possibilidades de combinações. Por causa dessa alta quantidade de possibilidades, o exército alemão considerou os benefícios em utilizar a "Enigma" para se comunicar com campo de batalha durante a Guerra, tornando a decodificação um verdadeiro desafio para seus inimigos.

2.4.1 Funcionamento da Máquina Enigma

A Máquina Enigma era portátil, ou seja, ela era carregada de forma fácil e funcionava por meio de uma série de componentes:

- **Livro:** Os operadores da máquina possuíam um livro com uma tabela inclusa para que cada dia do mês houvesse a indicação de qual dos 3 rotores deveria estar na máquina e suas devidas posições, assim como o posicionamento dos painéis de conexão.

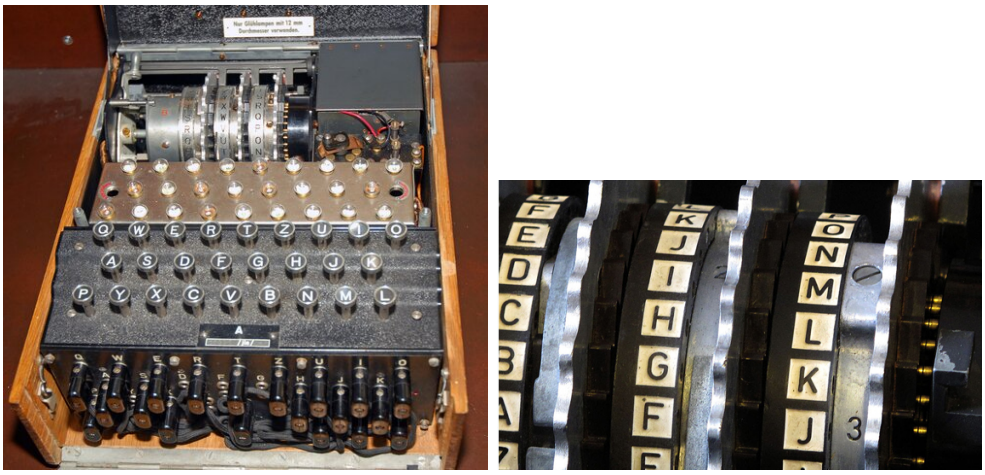
- **Rotores:** Escolher 3 dentre 5 discos rotativos que geravam uma substituição de letras diferente a cada clique na tecla. A rotação dos rotores criava um sistema de cifra polialfabética.

- **Painel de Plugs:** Antes delas entrarem nos rotores, havia a possibilidade de trocar as letras manualmente. Com 26 entradas equivalentes a cada letra do alfabeto e um fio conectando duas entradas. Com isso, cada par de plugs interligados alterava as letras. Criando assim, uma camada extra de codificação à cifra.

  Exemplo 2.4.1. *Se letra A fosse conectada à letra M, então pressionar A enviaria o sinal da letra M para os rotores, e pressionar M enviaria o sinal da letra A.*

- **Refletor:** Responsável por garantir que a mensagem cifrada fosse decodificada pelo receptor através do processo inverso dos rotores, refletindo a letra decifrada com um sinal luminoso. Todas as máquinas contavam com este componente, dando a elas a função de criptografar e descriptografar as mensagens com a mesma configuração.

Figura 5 – A Máquina Enigma e os 3 rotores.



Fonte: Disponível em: <https://www.tnmoc.org/bh-2-the-enigma-machine>. Acesso em: 31/08/2024.

2.4.2 The Bombe

Nascido em 1911, o britânico Alan Turing, que teve sua vida profissional retratada no filme “O jogo da imitação”, criou a The Bombe, a máquina responsável por quebrar a codificação da Enigma que é considerada pela ciência moderna um dos primeiros computadores criados. Contribuindo assim, com o fim da 2ª guerra mundial e salvando milhões de vidas. Por ter decodificado as mensagens enviadas, a máquina em questão, adiantou a guerra em 2 anos. O historiador David Kahn resume o impacto da quebra da Enigma:

> "Ela salvou vidas. Não apenas vidas aliadas e russas, ao encurtar a guerra, mas vidas alemãs, italianas e japonesas também. Algumas das pessoas que estavam vivas depois da Segunda Guerra Mundial não teriam sobrevivido se não fossem essas soluções. Esta é a dívida que o mundo tem para com os quebradores de códigos, este é o valor humano de seus triunfos." (SINGH, 2004).

2.4.3 **Colossus**

De acordo com PAIXÃO (PAIXãO, 2020), Hitler e seus generais confabulavam suas táticas de guerra usando uma máquina, mais complexa, a Lorenz. Então, Max Newman se baseou na máquina de Turing e projetou a "Colossus". Essa foi a máquina que motivou o progresso da criptografia na segunda metade do século XX. Mas, com sua missão cumprida e famosa pelo advento da guerra, o aparato e seus equipamentos foram destruídos entre 1945 e 1946, com o fim do conflito.

2.5 Curvas elípticas

Segundo Andrade (ANDRADE., 2016), a criptografia com uso de curvas elípticas foi, primeiramente, introduzida em 1985 por Victor Miller e Neal Koblitz, e vem sendo utilizada como uma nova forma de construção de sistemas de chave pública em algumas das aplicações já existentes. Esse método criptográfico ainda tem sido relevante nos últimos anos, porque está relacionado a gradativa necessidade de amparar a segurança dos modernos meios de comunicação, encontrado em tecnologias digitais onde a eficiência de processamento tem se atualizado a cada dia.

Os conteúdos matemáticos usados no sistema de criptografia aprendidos a partir das curvas elípticas são desenvolvidos sobre corpos finitos. Para tal, deve-se assumir conhecimentos de como grupos, anéis, corpos, estudado durante o curso de graduação em Matemática.

A vantagem do método de criptografia das curvas elípticas é a pequena extensão de suas chaves em relação às outras formas de criptografia mais utilizadas depois do surgimento dos computadores. Ela se torna mais eficiente por causa da menor ocupação de espaço de memória e o tempo gasto para ser processada e mesmo assim, mantém o mesmo nível de segurança oferecido pelo outro sistema de criptografia mais utilizado na atualidade, a RSA.

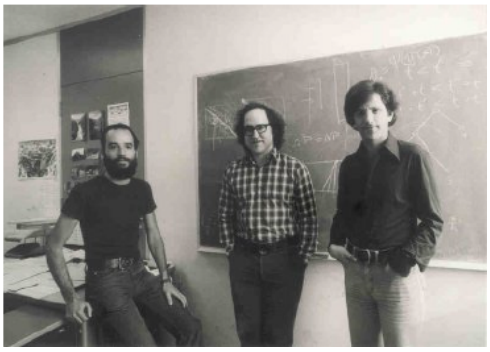
2.6 Criptografia RSA

Após a Segunda Guerra mundial, com a evolução dos computadores, ficou fácil quebrar todos os métodos de codificação vistos desde o início dos tempos. Por isso, houve

a necessidade de desenvolver táticas mais avançadas de cifragem.

Sendo publicada em 1978, a criptografia **RSA** é a junção da primeira letra do sobrenome de seus criadores, Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman. A ideia dos 3 cientistas foi fundamentada sobre uma das áreas mais clássicas do mundo da matemática, a teoria dos números, se baseando na dificuldade em decompor seus números astronômicos em fatores primos por causa do tempo gasto ao resolver a fatoração.

Figura 6 – Ronald Rivest, Adi Shamir e Leonard Adleman.



Fonte: Disponível em: <https://www.tnmoc.org/bh-2-the-enigma-machine>. Acesso em: 31/08/2024.

> "Foram Ronald Rivest, Adi Shamir e Leonard Adleman, do Laboratório de Ciências da Informação do Massachusetts Institute of Technology (MIT), que deram em 1978 o passo decisivo para a implementação do primeiro sistema criptográfico com chaves assimétricas, idealizado por Driffie. O princípio baseia-se na relativa facilidade de encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números, além do uso de propriedades relativamente elementares da Teoria dos Números" (HEFEZ, 2014).

Tudo que a ida é fácil e a volta é difícil, vira criptografia. Essa é a ideia central que reflete os algoritmos de criptografia nos dias de hoje, e ela se encaixa perfeitamente no conceito da criptografia RSA, que achar o resultado da multiplicação de dois números primos, é fácil, mas apenas saber o valor do produto para descobrir quem são os fatores, é difícil. Como pode ser observado no Exemplo 2.6.1, é notória a dificuldade de uma rede de computadores em fatorar números inteiros grandes.

Exemplo 2.6.1. *Segundo SINGH (SINGH, 2004), Em maio de 2007, um número inteiro de 1039 bits (Um bit é a menor unidade de informação em um sistema binário e pode ser 0 ou 1. Portanto, um número de 1039 bits é um número que, em binário, tem 1039 dígitos binários, cada um sendo 0 ou 1) foi fatorado com uso de 400 computadores levando 11 meses para chegar ao resultado da fatoração.*

2.6.1 Problemas futuros

A computação quântica pode trazer grandes novidades no quesito segurança da informação. Com ela, os métodos atuais de criptografia poderiam estar em risco com processamento muito maior e assim possibilita uma menor quantidade de tempo gasto para encontrar as chaves do método de criptografia RSA.

Ao longo dos próximos capítulos, será apresentado o funcionamento do algoritmo RSA, seu passo a passo até que seja alcançado o propósito deste trabalho que é a codificação e decodificação de uma informação.

3 Fundamentação teórica para a Criptografia RSA

Neste capítulo, damos um passo além da história da criptografia, explorando a conexão entre a matemática e a segurança digital. No capítulo anterior, vimos como a criptografia sempre foi uma ferramenta poderosa em contextos militares e políticos. Porém, com o avanço da tecnologia e o uso intenso de computadores por pessoas comuns, a criptografia moderna começou a ganhar um novo propósito: proteger a privacidade e a segurança das informações no dia a dia.

Uma parte importante desse avanço foi a criação da Criptografia RSA, um método que revolucionou a maneira como os dados são protegidos e por causa desse novo esquema, iremos nos aprofundar em alguns conceitos fundamentais da Teoria dos Números: números primos, fatoração, congruência entre outros conteúdos.

3.1 Divisibilidade

As propriedades de divisibilidade são conceitos fundamentais em aritmética e teoria dos números que ajudam a compreender quando um número pode ser dividido por outro sem deixar resto.

Definição 3.1.1. *Sejam a e b números inteiros. Diz-se que a divide b ou que a é divisor de b ou b é divisível por a ou b é múltiplo de a quando existe um número inteiro c tal que $b = a \cdot c$. Usa-se a notação $a|b$ para indicar que a divide b.*

Abaixo estão algumas propriedades, juntamente com suas respectivas demonstrações:

1. $a|1 \Rightarrow a = \pm 1$.

   Demonstração: Seja a um número inteiro tal que $a|1$. Então, existe um número inteiro b tal que $1 = a \cdot b$. Como $1 > 0$, então $a, b > 0$ ou $a, b < 0$. No caso em que $a, b > 0$, tem-se $a, b \geq 1$. Se ocorresse $a \geq 2$, então teríamos $1 = a \cdot b \geq 2b \geq 2 \cdot 1 = 2$, o que não é verdade. Logo, $a = 1$. No caso em que $a, b < 0$, tem-se $a, b \leq -1$. Se ocorresse $a \leq -2$, então teríamos $1 = a \cdot b \geq (-2)b \geq (-2)(-1) = 2$, o que não é verdade. Logo, $a = -1$.

2. Se $a, b \in \mathbb{Z}^+$, com $a > 0$, sendo $Z^+ = \{x \in \mathbb{Z}; x \geq 0\}$, e $b|a$, então $b \leq a$.

   Demonstração: Sejam $a, b \in \mathbb{Z}^+$, com $a > 0$, tais que $b|a$. Então, $a = k \cdot b$, para algum $k \in \mathbb{Z}$. Como $a, b \in \mathbb{Z}^+$, com $a > 0$, então $c > 0$. Assim, temos que $c \geq 1 \Rightarrow c \cdot b \geq 1 \cdot b \Rightarrow c \cdot b \geq b \Rightarrow a \geq b$. Portanto $b \leq a$.

3. Se $a|b$ e $b|a \Rightarrow b = \pm a$.

   Demonstração: Sejam $a, b \in \mathbb{Z}$ tais que $a|b$ e $b|a$. Então, existem $m, n \in \mathbb{Z}$ tais que $a = b \cdot m$ e $b = a \cdot n$. Assim, $b = a \cdot n = (b \cdot m)n = b(m \cdot n)$ e, portanto, $b(1 - m \cdot n) = 0$. Logo, $b = 0$ ou $mn = 1$. No caso em que $b = 0$, tem-se $a = bm = 0 \cdot m = 0$ e, logo, $b = 0 = \pm 0 = \pm a$. No caso em que $mn = 1$, tem-se que $m|1$ e, portanto, pelo item 1, segue que $m = \pm 1$. Se $m = 1$, então $a = b \cdot m = b \cdot 1 = b$ e, se $m = -1$, então $a = b \cdot m = b \cdot (-1) = -b$. Portanto, $b = \pm a$.

4. Se $a \neq 0$, então $a|0$.

   Como $a \in \mathbb{Z}$, podemos dizer que: $0 = 0 \cdot a$

5. Se $b|a$ e $a|c$, então $b|c$.

   Demonstração: Sejam $a, b, c \in \mathbb{Z}$, de maneira que: $a = mb$, para algum $m \in \mathbb{Z}$ e $c = na$, para algum $n \in \mathbb{Z}$, então, $c = n \cdot (mb) = (mn) \cdot b$, com $m, n \in \mathbb{Z}$. Portanto $b|c$.

6. Se a é divisível por b, então $k \cdot a$ é divisível por b para qualquer $k \in \mathbb{Z}$

   Demonstração: Se a é divisível por b, isso significa que existe um $m \in \mathbb{Z}$ tal que $a = b \cdot m$

   Multiplicando ambos os lados por k, temos: $k \cdot a = k \cdot (m \cdot b) = (k \cdot m) \cdot b$. Como $k \cdot m \in \mathbb{Z}$, isso prova que $k \cdot a$ é divisível por b.

7. $b|a$ e $b|c \Rightarrow b|(a \pm c)$.

   Demonstração: Provar que $b|a$ e $b|c$ implicam em $b|(a \pm c)$.

   Suponha que $b|a$ e $b|c$, então $a = b \cdot k_1$ e $c = b \cdot k_2$, para alguns inteiros k_1 e k_2.

   Considerando $a \pm c = b \cdot k_1 \pm b \cdot k_2 = b \cdot (k_1 \pm k_2)$, como $(k_1 \pm k_2)$ é um inteiro, isso prova que $b|(a \pm c)$

   Logo, $b|(a \pm c)$ quando $b|a$ e $b|c$.

8. Para quaisquer $m, n \in \mathbb{Z}$, temos que se $b|a$ e $b|c \Rightarrow b|(m \cdot a + n \cdot c)$.

   Suponha que $a = b \cdot k_1$, para algum inteiro qualquer $k_1 \in \mathbb{Z}$ e $c = b \cdot k_2$, para algum inteiro qualquer $k_2 \in \mathbb{Z}$. Logo, para algum inteiro qualquer $k_1 \in \mathbb{Z}$, $b \cdot k_3 = m \cdot a + n \cdot c \Rightarrow b \cdot k_3 = m \cdot (b \cdot k_1) + n \cdot (b \cdot k_2) \Rightarrow b \cdot k_3 = b \cdot (m \cdot k_1 + n \cdot k_2)$. Portanto, $b|(m \cdot a + n \cdot c)$.

3.2 Algoritmos

Conforme o leitor se aprofunda neste trabalho, ficará claro o papel essencial do algoritmo de divisão e do algoritmo euclidiano na compreensão da criptografia RSA. Esses

conceitos, descritos por volta de 300 a.C. nos Elementos de Euclides, envolvem o cálculo do quociente e do resto de uma divisão, além do método para determinar o máximo divisor comum entre dois números inteiros, aspectos que são cruciais para os fundamentos da criptografia moderna.

De acordo com Dicionário Houaiss da Língua Portuguesa (HOUAISS., 1986), a definição da palavra algoritmo é: "Conjunto finito de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas." Ou seja, a tarefa de um algoritmo é como seguir uma receita de bolo.

3.2.1 O algoritmo da divisão

Em primeiro lugar, para esta dissertação, interessa apenas a divisão de um inteiro positivo por outro para achar o quociente, também inteiro e positivo, e seu resto. Dito isso, imaginamos que o leitor pense nesta forma de divisão:

$$\begin{array}{r|l} 111 & 10 \\ \cline{2-2} 11 & 11 \\ 1 & \end{array}$$

Este exemplo ilustra a divisão de 111 por 10, resultando em um quociente de 11 e um resto de 1. Podemos identificar os demais elementos do algoritmo da divisão: o dividendo, 111 e o divisor, 10.

Sendo dividendo (D), divisor (d), quociente (q) e resto (r) os elementos do algoritmo da divisão. O leitor pode voltar no tempo e relembrar de seu Ensino Fundamental I, em que a professora utilizava de exemplo clássico como: "Tenho D balas e vou dividi-las de forma que meus d alunos recebam igualmente o maior número de balas possíveis". A resposta é que cada aluno vai receber uma quantidade q de balas e vai sobrar uma quantidade r de balas para professora. Pela proximidade com a realidade dos meninos, este tipo de problema é a forma mais simples de contextualizar o algoritmo da divisão para crianças.

No algoritmo da divisão, começamos com o dividendo e o divisor. A partir deles, conseguimos determinar, no final, os elementos que faltam, o quociente e o resto. De forma que todos se relacionam da seguinte maneira:

- **Preparação:** Verifique se o divisor é diferente de zero, porque a divisão por zero não está definida e compare o dividendo com o divisor. Se o dividendo for menor que o divisor, o quociente será 0 e o resto será o próprio dividendo.
- **Cálculo do Quociente (q):** Determine quantas vezes o divisor (d) cabe no dividendo (D).

- **Cálculo do Resto:** Calcular o resto (r) subtraindo o produto do divisor.

Teorema 3.2.1. *Sejam D e d números inteiros positivos. Existem inteiros q e r, tais que:*

$$D = d \cdot q + r, \text{ sendo } 0 \leq r < d. \tag{3.1}$$

Demonstração: Seja D e d números inteiros positivos. Se $D < d$, tomamos $q = 0$ e $r = D$. Se $D = d$, tomamos $q = 1$ e $r = 0$. Se $D > d$, tomamos q como sendo o maior número inteiro tal que $D \geq d \cdot q$, e tomamos r como sendo $r = D - dq$. Como $D \geq d \cdot q$, então $r = D - dq \geq 0$. Além disso, $r < d$. De fato, supondo, por absurdo, que $r \geq d$, ou seja, que $D - dq \geq d$, tem-se $D \geq d(q + 1)$ e, portanto, $q + 1$ é um número inteiro maior do que q e que multiplicado por d resulta ser menor do que ou igual a D, o que é um absurdo, uma vez que q é o maior número inteiro com essa propriedade. Logo, $r < d$.

Além disso, os valores de q e r satisfazendo as relações acima, são únicos.

Isso significa que para cada divisão, os valores do quociente e resto são determinados de forma única. A unicidade dos elementos revela que não importa o método utilizado para encontrá-los, sempre chegaremos aos mesmos valores, desde que as condições do teorema sejam respeitadas.

Com essa informação, vamos supor no exemplo que Rafael e Gabriel vão achar valores diferentes de quociente e resto numa divisão de mesmo dividendo e divisor.

Exemplo 3.2.2. *Rafael e Gabriel são irmãos gêmeos e a professora de matemática da dupla pediu para que cada um calculasse a divisão dos números inteiros e positivos D por d.*

Usando o Teorema 3.2.1 Rafael encontrou q e r e Gabriel q' e r':

Rafael: $D = d \cdot q + r$, *sendo* $0 \leq r < d$

Gabriel: $D = d \cdot q' + r'$, *sendo* $0 \leq r' < d$

Para provar a unicidade do quociente e resto, é necessário mostrar então que $q = q'$ e $r = r'$. Ao longo do texto foi dito que todos os números citados são inteiros. Portanto, r será maior que r' $(r \geq r')$ e para fixar a ideia, reescreveremos a equação do Teorema 3.2.1 de maneira que o resto esteja isolado.

Rafael: $r = D - d \cdot q$, sendo $0 \leq r < d$

Gabriel: $r' = D - d \cdot q'$, sendo $0 \leq r' < d$

Subtraindo uma equação da outra: $r - r' = (D - d \cdot q) - (D - d \cdot q') = d \cdot (q' - q)$

Supomos, por absurdo, que $r - r' \neq 0$, ou seja, que $r \neq r'$. Podemos supor, sem perda de generalidade, que $r > r'$, ou seja, que $r - r' > 0$. Como $r - r' = d(q' - q)$, então $d|(r - r')$. Como d e $r - r'$ são número inteiros positivos e $d|(r - r')$, então, pelo item

(2), $d \leq r - r'$. Mas, como $0 \leq r < d$ e $0 \leq r' < d$, então $r - r' < d - r' \leq d$ e, portanto, $r - r' < d$, o que não é absurdo, já que $d \leq r - r'$. Assim, $r = r'$. Como $r - r' = d(q' - q)$, $r - r' = 0$ e $d \neq 0$, então $q' - q = 0$ e, logo, $q = q'$.

Provando assim, a unicidade do teorema da divisão.

3.2.2 O algoritmo Euclidiano

O algoritmo Euclidiano tem como propósito encontrar o máximo divisor comum entre dois números inteiros e positivos. Nesta seção, abordaremos o que é o mdc e como ele deve ser entendido. Para isso, aplicaremos os conceitos já discutidos sobre o algoritmo da divisão, estudado no início deste capítulo.

Os livros de Ensino Fundamental II descrevem o estudo de máximo divisor comum de forma muito simples, porém ineficiente para a prática matemática na criptografia RSA. Por isso, a abordagem do método de Euclides neste trabalho é necessária para a definição do *mdc*.

Definição 3.2.3. *Dados os números $a, b, c, d \in \mathbb{Z}^+$. Para que o $mdc(a, b)$ seja d:*

1. *Quando $d|a$ e $d|b$, então isso significa que d é um divisor comum de a e b.*
2. *Quando $c|a$ e $c|b$, então $c|d$.*

O $mdc(a, b)$ é o maior divisor comum de a e b. De fato, seja d' o maior divisor comum de a e b. Como $d'|a$ e $d'|b$, então $d'|mdc(a, b)$ pela propriedade de divisibilidade no item (2), tem-se $d' \leq mdc(a, b)$. Por outro lado, como $mdc(a, b)|a$ e $mdc(a, b)|b$, então $mdc(a, b) \leq d'$. Logo, $mdc(a, b) = d'$.

A seguir, vamos apresentar um lema que será fundamental para demonstrar a existência do máximo divisor comum entre dois inteiros não negativos.

Lema 3.2.4. *Sejam $a, b, m \in \mathbb{Z}$, se $mdc(a, b - ma)$ existe, então $mdc(a, b)$ existe e $mdc(a, b) = mdc(a, b - ma)$.*

Demonstração: Seja $d = mdc(a, b - ma)$. Isso significa que d é um divisor comum de a e $b - ma$, ou seja, $d|a$ e $d|(b - ma)$. Podemos escrever b da seguinte maneira $b = b - ma + ma = dk_1 + ma \Rightarrow d|b$, para algum $k_1 \in \mathbb{Z}$. Logo $d|a$ e $d|b$.

Supondo que c seja divisor comum de a e b, então c também é divisor comum de a e $b - ma$. Portanto, $c|d$, provando que $d = mdc(a, b) = mdc(a, b - ma)$

Pela definição 3.2.3, se d é o maior divisor comum de a e b, então:

- d também divide $a \cdot x$, para algum inteiro x, pois considerando $a = d \cdot k_1$. Logo $d|(d \cdot k_1) \cdot x$.
- d também divide $b \cdot y$, para algum inteiro y, pois considerando $b = d \cdot k_2$. Logo $d|(d \cdot k_2) \cdot y$.
- Portanto, d divide a combinação linear $a \cdot x + b \cdot y$, pois $a \cdot x + b \cdot y = (d \cdot k_1) \cdot x + (d \cdot k_2) \cdot y = d \cdot (k_1 \cdot x + k_2 \cdot y)$. Mostrando assim que como $d|d \cdot (k_1 \cdot x + k_2 \cdot y)$, por transitividade, $d|a \cdot x + b \cdot y$

O algoritmo de Euclides é um método excepcional do ponto de vista computacional, e que mesmo após 2.000 anos, quase não precisou de melhorias, tamanha sua eficiência. Por causa de sua importância na área da computação e consequentemente utilização na criptografia moderna, ele será mostrado, de forma sintética, utilizando o algoritmo da divisão e a Tabela 7, que será iniciado com a divisão $a = b \cdot q_1 + r_1$, sendo os quocientes e restos expressos respectivamente por q_i e r_i, prosseguindo com as sucessivas divisões, até encontrar $n \in N$, tal que $r_n|r_{n-1}$ (em outras palavras, $r_{n+1} = 0$):

Tabela 7 – Diagrama para efetuar o algoritmo de Euclides.

	q_1	q_2	q_3	q_4	q_5	...	q_n	q_{n+1}
a	b	r_1	r_2	r_3	r_4	...	r_{n-1}	$r_n = mdc(a,b)$
r_1	r_2	r_3	r_4	r_5	r_6	...	$r_{n+1} = 0$	

Fonte: Produção da própria autora, inspirada por HEFEZ (HEFEZ, 2014).

Nada melhor que um exemplo para compreender o método de Euclides:

Exemplo 3.2.5. *Vamos calcular o* $mdc(a,b)$*, onde* $a = 1110$ *e* $b = 11$*:*

Tabela 8 – Cálculo do $mdc(1110, 11)$.

	100	1	10
1110	11	10	$1 = mdc(1110, 11)$
10	1	0	

Fonte: Produção da própria autora

Ao analisar os restos obtidos pelo algoritmo na Tabela 8, observamos o seguinte:

$1 = 11 - 10 \cdot 1$

$10 = 1110 - 11 \cdot 100$

Substituindo os valores encontrados:

$1 = 11 - 10 \cdot 1 = 11 - (1110 - 11 \cdot 100) \cdot 1 = 11 - 1110 + 11 \cdot 100 = 11 \cdot 101 - 1110 \cdot 1$

Além de calcular o máximo divisor comum entre dois números inteiros (garantindo a sua existência), o Algoritmo de Euclides também serve como uma ferramenta poderosa para expressar esse mdc como uma combinação linear de múltiplos de dois números, a e b. Como vimos na análise dos restos feita anteriormente, podemos escrever que $mdc(1110, 11) = 1 = 101.11 + (-1).1110$. Essa técnica de representar o $mdc(a, b)$ como $x \cdot a + y \cdot b$, onde $x, y \in \mathbb{Z}$, é mais eficaz que o método utilizado no Ensino Fundamental II e é conhecida como o Algoritmo Estendido de Euclides.

Demonstração do Algoritmo Estendido de Euclides: Dados dois números inteiros a e b, com $0 < b \leq a$, o Algoritmo de Euclides nos permite encontrar o mdc de a e b por meio de cálculos baseado em termos obtidos em passos anteriores. O Algoritmo de Euclides Estendido vai além, permitindo expressar o *mdc* como uma combinação linear dos números a e b, ou seja:

$$mdc(a, b) = x \cdot a + y \cdot b, \text{onde } x, y \in \mathbb{Z}. \tag{3.2}$$

Como já dito anteriormente a divisão de a por b pode ser expressa da seguinte forma:

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$.$$

$$.$$

$$.$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$

$$r_{n-1} = r_n \cdot q_{n+1} + 0$$

Aqui, $r_n = mdc(a, b)$. A última equação será a primeira onde o resto se torna zero, ou seja, a equação que fornece o máximo divisor comum.

Agora, podemos "voltar" substituindo os valores dos restos anteriores, a partir da equação final.

- Sabendo que $r_n = mdc(a, b)$.
- Usando a penúltima equação: $r_{n-2} = r_{n-1} \cdot q_n + r_n$
- Mas $r_{n-3}, r_{n-4}, \ldots, b, a$ também podem ser escritos em termos dos restos anteriores. Continuando assim, substituindo recursivamente até que os restos sejam escritos em termos de a e b.

O Algoritmo de Euclides Estendido consiste em encontrar o *mdc* de a e b usando divisões sucessivas e, ao voltar, reescrever o *mdc* como uma combinação linear de a e b. A chave da demonstração está no fato de que, em cada etapa, expressamos os restos como combinações lineares dos números originais, até que, no final, o *mdc* seja escrito nessa forma.

Quando o *mdc* entre dois números é igual a 1, dizemos que eles são primos entre si, porque não tem múltiplos em comum. Vamos analisar a seguinte proposição e demonstrá-la:

Proposição 3.2.6. *Dois números $a, b \in \mathbb{Z}$ são coprimos se, somente se, existem $x, y \in \mathbb{Z}$ tais que $x \cdot a + y \cdot b = 1$.*

Demonstração:

Ida: Se $mdc(a, b) = 1$, então existem $x, y \in \mathbb{Z}$ tais que $x \cdot a + y \cdot b = 1$.

Sabemos que o Algoritmo de Euclides Estendido nos permite calcular o *mdc* de dois números inteiros a e b, e expressar esse *mdc* como uma combinação linear de a e b.

Se $mdc(a, b) = 1$, o Algoritmo de Euclides Estendido nos diz que podemos escrever o *mdc* na forma: $x \cdot a + y \cdot b = 1$, onde x e y são inteiros, que podem ser obtidos a partir da substituição dos restos no processo do algoritmo. Isso prova que, se a e b são coprimos, ou seja, $mdc(a, b) = 1$, então existem inteiros x e y que satisfazem a equação.

Volta: Se existe $x, y \in \mathbb{Z}$ tais que $x \cdot a + y \cdot b = 1$. Então $mdc(a, b) = 1$.

Supomos que existam $x, y \in \mathbb{Z}$ tais que $x \cdot a + y \cdot b = 1$ e que seja $d = mdc(a, b)$. De acordo com as propriedades de divisão já demonstradas no início deste capítulo, quando d divide tanto a quanto b, ele deve dividir qualquer combinação linear de a e b. Portanto, d deve dividir $x \cdot a + y \cdot b$ e $x \cdot a + y \cdot b = 1$. Logo, d divide 1 e o único divisor positivo de 1 é 1, então $d = 1$. Ou seja, por transitividade $mdc(a, b) = 1$. O que prova que a e b são coprimos.

3.3 Números primos e compostos

Afim de melhorar nossa compreensão sobre criptografia moderna, estudaremos sobre números primos e sua natureza que é capaz de produzir todos os demais números naturais. Quando se fala sobre a decomposição de números naturais em fatores primos, é importante recordar a definição de um número primo.

Definição 3.3.1. *Um número natural $p > 1$ é um número primo se, e somente se, seus únicos divisores positivos forem 1 e ele mesmo.*

Um número inteiro p é considerado primo se p é diferente de ± 1 e os únicos dois divisores de p são 1 e p. Isso significa que números como $2, 3, 5, 7, 11$ e 13 são primos,

porque não podem ser divididos por nenhum outro número além desses. O número 1 não é considerado primo, pois 1 só possui um divisor natural, no caso ele mesmo. Além do 1, temos outros exemplos, como o número 35, que pode ser escrito como $5 \cdot 7$, ou seja, não é primo, já que possui divisores além do próprio ± 1 e ± 35. Um número natural que não é primo e não é igual a 1 é chamado de número composto. Portanto, pode-se afirmar que 35 é um número composto.

Todo número natural $N \neq 1$ e $N \neq 0$ pode ser escrito na forma:

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_t}, \tag{3.3}$$

ou seja, decomposto em fatores primos.

Lema 3.3.2. *(Lema de Gauss) Se a, b e c são números inteiros tais que $a|(bc)$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração: Como $mdc(a, b) = 1$, então existem números inteiros r e s tais que $1 = ra + sb$ e, portanto, $c = rac + sbc = (rc)a + (s)bc$. Como $c = (rc)a + (s)bc$, $a|a$ e $a|(bc)$, então, pela propriedade da divisibilidade 8, tem-se que $a|c$.

Lema 3.3.3. *(Lema de Euclides) Se a e b são números inteiros e p é um número primo tal que $p|(ab)$, então $p|a$ ou $p|b$.*

Demonstração: Se $mdc(p, a) > 1$, então $p|a$, já que p é primo. Se $mdc(p, a) = 1$, então, pelo Lema 3.3.2, de Gauss, como $p|(ab)$, segue que $p|b$. Assim, $p|a$ ou $p|b$.

Teorema 3.3.4. *Teorema Fundamental da Aritmética Todo número Natural N, tal que $N > 1$, é primo ou se escreve de forma exclusiva, como um produto de números primos.*

Demonstração: O Teorema Fundamental da Aritmética afirma que todo número inteiro $N > 1$ pode ser escrito de forma única como um produto de números primos, exceto pela ordem dos fatores. Abaixo, faremos uma demonstração desse teorema por indução sobre N.

Para formalizar, queremos mostrar que:

1. **Existência**: Todo $N > 1$ pode ser escrito como um produto de números primos.

   (i) Para $N = 2$, vemos que 2 é um número primo. Logo, 2 pode ser escrito como o produto de apenas um número primo: ele mesmo. A proposição é verdadeira para $N = 2$.

   (ii) Supondo que $p(N)$ é verdade, vamos provar que $N + 1$ também pode ser escrito como um produto de números primos.

- **Caso 1**: Se $N + 1$ é um número primo, então ele já está escrito como um produto de primos (ele mesmo).
- **Caso 2**: Se $N + 1$ não é primo, então ele é composto e pode ser escrito como o produto de dois inteiros a e b, onde $2 \leq a, b < N + 1$.

  Como a e b são menores que $N + 1$, a hipótese de indução garante que ambos podem ser decompostos em fatores primos. Logo, podemos escrever $N+1 = a \cdot b$ como o produto de primos, por ser o produto das decomposições em primos de a e b.

Portanto, $p(N)$ é válido implica na validez de $p(N + 1)$. Conclusão: Todo número natural $N > 1$ pode ser escrito como um produto de números primos.

2. **Unicidade**: Essa decomposição é única, salvo pela ordem dos fatores.

   Para provar a unicidade da decomposição em fatores primos, utilizaremos um argumento por contradição.

   Supondo, por contradição, que existe um número N que pode ser escrito como dois produtos diferentes de números primos:

$$N = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \tag{3.4}$$

   onde p_i e q_j são números primos e as duas sequências de primos $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_m$ são distintas.

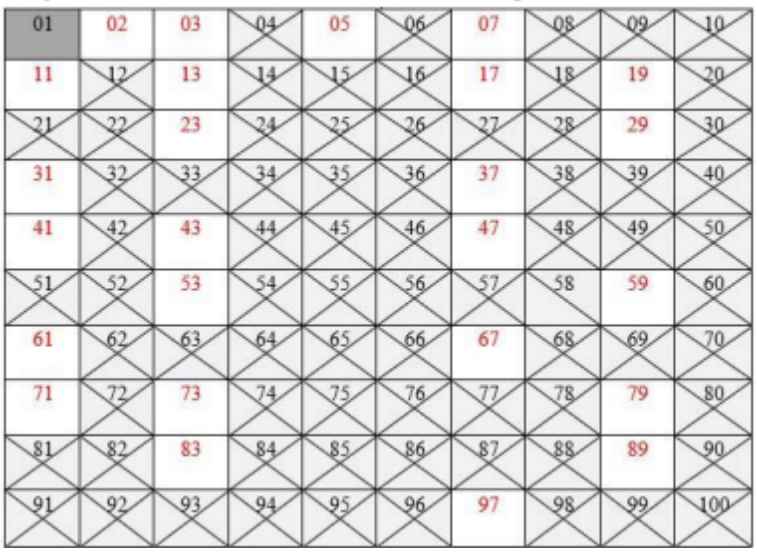
   ABSURDO! Pelo Lema 3.3.3, de Euclides, qualquer número primo que divide um produto de números deve dividir pelo menos um dos fatores. Isso implica que p_1 deve dividir algum q_j e, como q_j é primo, isso significa que $p_1 = q_j$. Repetindo o argumento para os demais primos, podemos cancelar todos os p_i e q_j, mostrando que as duas decomposições devem ter exatamente os mesmos fatores primos, possivelmente em uma ordem diferente.

   Portanto, foi mostrado que a decomposição de N em fatores primos é única, salvo pela ordem dos fatores.

Com isso, foi demonstrado o Teorema Fundamental da Aritmética: todo número inteiro $n > 1$ pode ser escrito de forma única (exceto pela ordem dos fatores) como um produto de números primos.

O Crivo de Eratóstenes, encontrado na Figura 7 é um algoritmo eficiente para encontrar todos os números primos até um certo número natural n qualquer. Ele funciona de maneira a criar uma lista de números do 2 até o n. Após essa anotação, será riscado todos os múltiplos do 2 que estiver na lista, exceto o próprio 2. O processo irá se repetir

Figura 7 – Crivo de Eratóstenes.



Fonte: (LIMA, 2024, p. 6)

com o próximo primo, que no caso é o 3. A técnica continua até ser processado todos os $n-1$ números e os que não estiverem riscados nesta lista são os primos.

Teorema 3.3.5. *Existem infinitos números primos.*

Uma das demonstrações mais conhecidas foi apresentada por Euclides que será apresentada abaixo numa versão simplificada.

Demonstração: Supondo por contradição que existe um número finito de números primos. Vamos listar todos os números primos conhecidos:

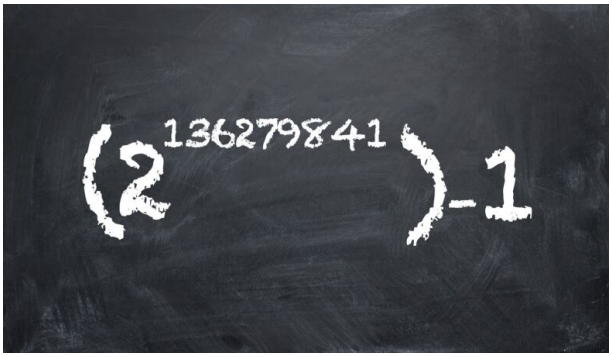
$$p_1, p_2, p_3, \ldots, p_n. \tag{3.5}$$

Considere o número N definido como $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$. Isso significa que o número N não pode ser divisível por nenhum dos primos listados, pois, se dividirmos N por qualquer primo p_i, teremos um resto de 1. Ou seja, N não é divisível por nenhum dos primos que listamos. Assim, existem duas possibilidades:

- N é um número primo, diferente de todos os primos da nossa lista.
- N é composto, mas N deve ter pelo menos um fator primo que não está na listagem de primos já conhecidos, pois não é divisível por nenhum deles.

Em ambos os casos, isso leva a uma contradição com a suposição de que havia um número finito de primos. Portanto, foi mostrado a infinidade de números primos, como queríamos demonstrar.

Figura 8 – Maior número primo já descoberto.



Fonte: Disponível em: <https://zap.aeiou.pt/maior-primo-descoberto-636200>. Acesso em 25/02/2025

De acordo com LEVENIUS (LEVENIUS, 2024), o maior número primo já descoberto, em outubro de 2024, é $2^{136.279.841} - 1$, que possui 41.024.320 algarismos. Este número foi encontrado por Luke Durant, um ex-programador da Nvidia, no projeto Great Internet Mersenne Prime Search (GIMPS). Este número pertence à sequência números dos primos de Mersenne, que são números primos da forma $2^p - 1$, onde p também é um primo.

3.4 Mínimo múltiplo comum (MMC)

No Ensino Básico, chamamos de Mínimo Múltiplo Comum (MMC) de a e b o menor número natural m que é múltiplo comum de ambos, considerando que a e b são diferentes de zero. Denotamos o mínimo múltiplo comum de a e b como $mmc(a, b)$. No Ensino Superior, a definição é um pouco mais formal:

Definição 3.4.1. *O número inteiro positivo m é um mínimo múltiplo comum dos números inteiros a e b (escreve-se $m = mmc(a, b)$) quando:*

1. *m é múltiplo comum de a e b.*
2. *$c \in \mathbb{Z}$ é um múltiplo comum de a e b, logo $m|c$.*

Como $mmc(a, b)$ divide qualquer múltiplo comum de a e b, então $mmc(a, b)$ é o menor múltiplo comum positivo de a e b.

Para mostrar que um número m que satisfaz as condições acima existe. Considera-se a decomposição de a e b em fatores primos:

Supondo que a e b têm decomposições em fatores primos dadas por:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \text{ e } b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}, \tag{3.6}$$

onde $p_1, p_2, \ldots, p_k$ são os fatores primos comuns ou distintos entre a e b (para primos que não aparecem em um dos números, consideramos o expoente igual a zero).

Definimos m como:

$$m = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}. \tag{3.7}$$

Esse número m é divisível tanto por a quanto por b, pois cada fator primo aparece em m com o maior expoente encontrado nas decomposições de a e b .

Unicidade: Suponha, por absurdo, que existam dois mínimos múltiplos comuns de a e b diferentes, digamos que sejam m_1 e m_2. Ambos satisfazendo as condições de divisibilidade e minimalidade, significa dizer que m_1 é múltiplo de a e b. Como m_2 também é múltiplo de a e b, m_2 será divisível por qualquer outro múltiplo comum de a e b, assim $m_2|m_1$. Com um raciocínio análogo, temos $m_1|m_2$ e pela propriedade de divisibilidade 3 demonstrada neste mesmo capítulo, pode-se concluir que $m_1 = m_2$, contradizendo a hipótese inicial que supõe dois mínimos múltiplos comuns diferentes, mostrando assim a unicidade.

Proposição 3.4.2. *Dados $a, b \in \mathbb{Z}$, então existe o mínimo múltiplo comum $mmc(a, b)$ e temos que:*

$$mmc(a, b) \cdot mdc(a, b) = |ab|. \tag{3.8}$$

Demonstração: Supondo que a e b possuem as seguintes decomposições em fatores primos:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \text{ e } b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}, \tag{3.9}$$

onde $p_1, p_2, \ldots, p_k$ são os fatores primos de a e b, e $\alpha_i, \beta_i \geq 0$ são os respectivos expoentes.

Por definição, o $mdc(a, b)$ e o $mmc(a, b)$ podem ser escritos respectivamente como:

$$\begin{aligned} mdc(a, b) &= p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)} \text{ e} \\ mmc(a, b) &= p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}. \end{aligned}$$

Isso implica que produto de $mdc(a, b)$ e $mmc(a, b)$ é:

$$mdc(a, b) \cdot mmc(a, b) = \left(p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}\right) \cdot \left(p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}\right)$$

$$mdc(a, b) \cdot mmc(a, b) = p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)+\max(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)+\max(\alpha_k,\beta_k)}$$

e simplificando o produto usando a propriedade $\min(x, y) + \max(x, y) = x + y$, obtemos:

$$mdc(a, b) \cdot mmc(a, b) = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_k^{\alpha_k+\beta_k} = |ab|. \tag{3.10}$$

Portanto, foi mostrado que $mdc(a, b) \cdot mdc(a, b) = |ab|$, como queríamos demonstrar.

A existência do $mmc(a, b)$ é garantida pelo fato de $mmc(a, b) \cdot mdc(a, b) = |ab|$, ou seja, o número inteiro positivo k que satisfaz $k \cdot mdc(a, b) = |ab|$ é o $mmc(a, b)$.

Corolário 3.4.3. *Dados $a, b \in \mathbb{Z}$, tal que $mdc(a, b) = 1$, então $mmc(a, b) = |ab|$.*

Demonstração: Se $mdc(a, b) = 1$, então como já demonstrado na Proposição 3.4.2 que $mmc(a, b) \cdot mdc(a, b) = |ab| \Rightarrow mmc(a, b) \cdot 1 = |ab| \Rightarrow mmc(a, b) = |ab|$.

Portanto, foi mostrado que se $mdc(a, b) = 1$, então $mmc(a, b) = |ab|$, como queríamos mostrar.

Para melhor visualização, a Proposição 3.4.2 e Corolário 3.4.3 serão exemplificados a seguir:

Exemplo 3.4.4. *Sejam $a = 11$ e $b = 111 = 3 \cdot 37$, logo o $mdc(11, 111) = 1$, ou seja, são coprimos, e $mmc(11, 111) = 3 \cdot 11 \cdot 37 = 1221$. Então, $mmc(11, 111) \cdot mdc(11, 111) = 1221 \cdot 1 = 1221$*

Proposição 3.4.5. *Propriedade Associativa do mmc*

$$mmc(a_1, \cdots, a_{n-1}, a_n) = mmc(a_1, \cdots, mmc(a_{n-1}, a_n)). \tag{3.11}$$

Demonstração: De acordo com (HEFEZ, 2014), se a igualdade acima existe, ela pode ser provada por indução: Vamos provar, por indução, que

$$mmc(a_1, \ldots, a_{n-1}, a_n) = mmc(a_1, \ldots, \text{mmc}(a_{n-1}, a_n)).$$

Base da Indução

Para $n = 2$, a afirmação é diretamente válida, pois:

$$mmc(a_1, a_2) = mmc(a_1, mmc(a_2)) = mmc(a_1, a_2).$$

Ou seja, a sentença é válida!

Hipótese de Indução

Supondo que $p(n) : mmc(a_1, \ldots, a_{n-1}, a_n) = mmc(a_1, \ldots, mmc(a_{n-1}, a_n))$ seja verdade, então $n + 1$:

O que precisamos provar: $mmc(a_1, \ldots, a_n, a_{n+1}) = mmc(a_1, \ldots, mmc(a_n, a_{n+1}))$.

Pela definição de mmc, a operação é associativa, ou seja:

$$mmc(a, mmc(b, c)) = mmc(mmc(a, b), c).$$

Aplicando isso no contexto da hipótese de indução:

1. Pela hipótese de indução, sabemos que:

$$mmc(a_1, \ldots, a_n) = mmc(a_1, \ldots, mmc(a_{n-1}, a_n)).$$

2. Agora, adicionando a_{n+1} no cálculo, obtemos:

$$mmc(a_1, \ldots, a_n, a_{n+1}) = mmc(mmc(a_1, \ldots, a_n), a_{n+1}).$$

   O que está sendo afirmado é uma aplicação da associatividade do mmc e que podemos tratar $mmc(a_1, \ldots, a_n)$ como um "único número" e calcular o mmc desse número com a_{n+1}.

3. Substituímos a hipótese de indução no lugar de $mmc(a_1, \ldots, a_n)$:

$$mmc(a_1, \ldots, a_n, a_{n+1}) = mmc(mmc(a_1, \ldots, mmc(a_{n-1}, a_n)), a_{n+1}).$$

4. Pela associatividade do mmc:

$$mmc(mmc(a_1, \ldots, mmc(a_{n-1}, a_n)), a_{n+1}) = mmc(a_1, \ldots, mmc(a_n, a_{n+1})).$$

   Portanto, pelo princípio da indução matemática, a propriedade

$$mmc(a_1, \ldots, a_{n-1}, a_n) = mmc(a_1, \ldots, mmc(a_{n-1}, a_n))$$

é verdadeira, implicando na validez de $p(n+1)$ para todo $n \geq 2$.

3.5 Equações Diofantinas Lineares

Nesta seção, será estudado a respeito das resoluções de equações diofantinas lineares. Equações diofantinas são equações do tipo $ax + by = c$, onde $a, b, c \in \mathbb{Z}$ e são os coeficientes da equação. Suas soluções são caracterizadas por terem mais de um valor inteiro para x e y.

De acordo com HARDY (HARDY., 2008) e DAVENPORT (DAVENPORT., 2000), as equações diofantinas são equações nas quais se procura descobrir respostas com números inteiros ou racionais. Elas foram nomeadas em tributo a Diofanto de Alexandria, que solucionou problemas desse tipo na Antiguidade. O estudo das equações diofantinas é um dos ramos primordiais da teoria dos números, englobando desde casos simples, como as equações lineares, até problemas mais difíceis, como o Último Teorema de Fermat. As maneiras de solucionar variam desde métodos utilizando álgebra clássica até avanços da modernidade envolvendo teoria dos grupos, curvas elípticas e algoritmos computacionais.

Já começando os estudos acerca do tema, é possível afirmar que algumas equações diofantinas não possuem soluções que pertencem ao conjunto dos números inteiros. A seguir, será abordado um exemplo trivial, ou seja, que não exige grandes conhecimentos sobre o passo a passo para encontrar as soluções.

Exemplo 3.5.1. $2x + 4y = 5$

Não possui solução no conjunto dos inteiros, porque como 2 *e* 4 *são números pares, os resultados encontrados para qualquer combinação* $2x + 4y$ *também será par, ou seja, nunca poderá ser 5 que é um número ímpar.*

Exemplo 3.5.2. *Em contrapartida, temos outros exemplos com variadas soluções para apenas uma equação. Como é apresentado na seguinte equação:*

$$2x + 3y = 6 \tag{3.12}$$

Com algumas soluções expostas:

$$2 \cdot 3 + 3 \cdot 0 = 6$$

$$2 \cdot 0 + 3 \cdot 2 = 6$$

$$2 \cdot 6 + 3 \cdot (-2) = 6$$

A condição de existir soluções para equação se promove através da proposição para determiná-la.

Proposição 3.5.3. *Critério de existência de soluções em equações diofantinas. Sejam* $a, b, c \in \mathbb{Z}$*, temos que a equação* $aX + bY = c$*, admite solução se, e somente se,* $mdc(a, b)|c$.

Demonstração:

Ida: Se existe solução de $ax + by = c$, então $mdc(a, b)|c$.

Considere que se $mdc(a, b) = d$, então $a = dm$ e $b = dn$, sendo $m, n \in \mathbb{Z}$.

Por hipótese temos que $ax + by = c$ e por transitividade é possível reescrever a equação na forma $(dm) \cdot x + (dn) \cdot y = c \Rightarrow d(mx) + d(ny) = c \Rightarrow d(mx + ny) = c$. Portanto, $d|c$

Volta: Se $d|c$, então existe solução para equação $ax + by = c$.

Sabemos que o Algoritmo de Euclides Estendido permite calcular o mdc de dois números inteiros a e b, e expressar esse mdc como uma combinação linear de a e b, ou seja, $x_0 \cdot a + y_0 \cdot b = d$. Como, por hipótese $d|c$, a expressão pode ser escrita da maneira $c = dt$, sendo $t \in \mathbb{Z}$. Assim, $x_0 \cdot a + y_0 \cdot b = d \Rightarrow (x_0 \cdot a + y_0 \cdot b) \cdot t = d \cdot t = c \Rightarrow x_0 t \cdot a + y_0 t \cdot b = c$, onde x_0 e y_0 são inteiros. Então, basta definir $x = x_0 t$ e $y = y_0 t$. Portanto, $ax + by = c$. Como queríamos mostrar.

Proposição 3.5.4. *Se x_0, y_0 é uma solução particular da equação $aX + bY = c$, no qual o $mdc(a, b) = 1$. Então, as possíveis soluções para $x, y \in \mathbb{Z}$ são:*

$$\begin{cases} x = x_0 + t \cdot b, \\ y = y_0 - t \cdot a \end{cases}, \ t \in \mathbb{Z} \tag{3.13}$$

Demonstração: Como, por hipótese, o par x_0, y_0 é solução particular da equação $aX + bY = c$, então $aX_0 + bY_0 = c$, logo, por transitividade, a equação pode ser escrita na forma $aX + bY = aX_0 + bY_0 \Rightarrow aX - aX_0 = bY_0 - bY \Rightarrow a(X - X_0) = b(Y_0 - Y)$. Como, também por hipótese, $a \nmid b$ e $b \nmid a$, porque $mdc(a, b) = 1$, então:

$$b|(X - X_0) \text{ e } a|(Y_0 - Y)$$
$$b \cdot t_1 = (X - X_0) \text{ e } a \cdot t_2 = (Y_0 - Y)$$
$$X = X_0 + b \cdot t_1 \text{ e } Y = Y_0 - a \cdot t_2,$$

sendo t_1 e t_2 constantes pertencentes ao conjunto dos números inteiros. Assim,

$$aX = aX_0 + ab \cdot t_1 \text{ e } bY = bY_0 - ab \cdot t_2$$

e somando as equações obtemos

$$aX + bY = aX_0 + bY_0 + ab \cdot (t_1 - t_2).$$

Como o par x, y é uma solução qualquer da equação, ficamos com

$$c = c + ab \cdot (t_1 - t_2) \Rightarrow ab \cdot (t_1 - t_2) = 0 \Rightarrow t_1 = t_2.$$

De modo que a proposição fica demonstrada tomando $t_1 = t_2$.

Exemplo 3.5.5. *Uma aplicação prática da demonstração da Proposição 3.5.4 é a resolução da equação $24x - 14y = 18$.*

Tabela 9 – Cálculo do $mdc(24, 14)$.

	1	1	2	2
24	14	10	4	$2 = mdc(24, 14)$
10	4	2	0	

Fonte: Produção da própria autora

A equação diofantina possui solução, porque $mdc(24, 14) = 2$ e $2|18$, porém como o $mdc(24, 14) \neq 1$, para que o exemplo se encaixe na Proposição 3.5.4, a equação pode ter seus dois membros simplificado por 2:

$$\frac{24x - 14y}{2} = \frac{18}{2}$$
$$12x - 7y = 9$$

Tabela 10 – Cálculo do $mdc(12, 7)$.

	1	1	2	2
12	7	5	2	$1 = mdc(12, 7)$
5	2	1	0	

Fonte: Produção da própria autora

Com a ajuda do algoritmo do $mdc(12, 7)$*, será permitido achar a solução particular da equação,* x_0, y_0*.*

$$1 = 5 - 2 \cdot 2$$
$$2 = 7 - 5 \cdot 1$$
$$5 = 12 - 7 \cdot 1$$

$$\begin{aligned} 1 = 5 - 2 \cdot 2 &= 5 - 2 \cdot (7 - 5 \cdot 1) \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (12 - 7 \cdot 1) - 2 \cdot 7 \\ &= 3 \cdot 12 - 3 \cdot 7 - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 \end{aligned}$$

$$(3 \cdot 12 - 5 \cdot 7) \cdot 9 = 1 \cdot 9$$
$$27 \cdot 12 - 45 \cdot 7 = 9$$

Portanto, $(x_0, y_0) = (27, 45)$ *é uma solução particular da equação.*

Logo, as demais soluções podem ser escritas na forma $x = 27 - 7t$ *e* $y = 45 - 12t$*, com* $t \in \mathbb{Z}$ *de acordo com a Proposição 3.5.4.*

Conjunto das lacunas: Se uma sequência de números naturais é um subconjunto próprio de $\{n \in \mathbb{N} \,|\, n_0 \leq n \leq n_1 \text{ com } n_0, n_1 \in \mathbb{N}\}$, o conjunto das lacunas seria o complemento deste conjunto formado pelos números que **não** estão presentes na série.

Exemplo 3.5.6. *Se temos a sequência de números naturais:* $\{1, 2, 3, 5, 6, 8\}$*, o conjunto das lacunas seria* $\{4, 7\}$*, porque são os dois números ausentes na sequência.*

A sua aplicação na criptografia, o conjunto das lacunas pode ser empregado em intervalos de chaves de números inteiros possíveis.

Teorema 3.5.7. *A equação $aX + bY = c$, com $mdc(a, b) = 1$ tem solução em $N \cup \{0\}$ se, e somente se $c \notin \ell(a, b) = \{na - mb; n, m, na - mb \in \mathbb{N}, n < b\}$.*

Demonstração:

Ida: Se $aX + bY = c$, com $mdc(a, b) = 1$ tem solução em $N \cup \{0\}$, então $c \notin \ell(a, b) = \{na - mb; n, m, na - mb \in \mathbb{N}, n < b\}$.

- A condição de $mdc(a, b) = 1$, implica no critério de existência de soluções em equações diofantinas demonstrado na Proposição 3.5.3, que enuncia que se c é múltiplo de $mdc(a, b)$ a equação tem pares soluções pertencente ao conjunto dos números inteiros.
- No entanto, a questão não é apenas sobre existência em $\mathbb{Z}$, mas em $N \cup \{0\}$. Para que $c \notin \ell(a, b)$ é preciso que ele não seja escrito na forma $na - mb; n, m, na - mb \in \mathbb{N}, n < b$.
- Suponha, por contradição, que $c \in \ell(a, b)$. Logo, pode-se dizer que existe $c = na - mb; n, m, na - mb \in \mathbb{N}, n < b$. Entretanto, neste caso, $aX + bY = c$, não teria solução em $N \cup \{0\}$, porque os valores de x e y necessários para que satisfaça a equação dependem de m e n que estão em $\ell(a, b)$

Volta: Se $c \notin \ell(a, b) = \{na - mb; n, m, na - mb \in \mathbb{N}, n < b\}$, então a equação $aX + bY = c$, com $mdc(a, b) = 1$ tem solução em $N \cup \{0\}$.

- Se $c \notin \ell(a, b)$, então os valores de x e y devem ser ajustados com os valores de t, de acordo com a solução geral da equação citada na proposição 3.5.4, de forma que eles não sejam inteiros negativos

$$\begin{cases} x = x_0 + t \cdot b, \\ y = y_0 - t \cdot a \end{cases}, \ t \in \mathbb{Z}.$$

- Assim, $c \notin \ell(a, b)$ implica que existe pelo menos uma escolha de t que garante que x e $y \in N \cup \{0\}$

Corolário 3.5.8. *Sejam $a, b \in \mathbb{N}$ tais que $mdc(a, b) = 1$. Tem-se que $(a - 1) \cdot (b - 1)$ é o menor valor inteiro c que admite solução. Ou seja, $c \geq (a - 1) \cdot (b - 1)$*

Demonstração: Note que quando n for máximo, isto é, $n = b - 1$ e m for mínimo, ou melhor dizendo, $m = 1$. O conjunto das lacunas terá seu maior elemento:

$$\max \ell(a, b) = ab - a - b$$

$$\max \ell(a, b) = (b - 1) \cdot a - b$$

$$c \geq (b-1) \cdot a - b+1$$

$$c \geq (a-1) \cdot (b-1)$$

Portanto, se $c \geq (a-1) \cdot (b-1)$ a equação admite soluções nos naturais.

Exemplo 3.5.9. *Determinar para quais valores de c a equação* $7x + 5y = c$ *tem solução no conjunto* $N \cup \{0\}$*:*

Tabela 11 – Cálculo do $mdc(5, 7)$.

	1	2	2
7	5	2	$1 = mdc(7, 5)$
2	1	0	

Fonte: Produção da própria autora

$1|c$*, logo a equação tem solução!*

O conjunto das lacunas é $\ell(7, 5) = \{7n - 5m; m, n, 7m - 5n \in \mathbb{N}, n < 5\}$ *e seu maior elemento é* $(7-1) \cdot (5-1) - 1 = 6 \cdot 4 - 1 = 24 - 1 = 23$

Tabela 12 – Tabuada do 7 e 5.

$7 \cdot 1 = 7$	$5 \cdot 1 = 5$
$7 \cdot 2 = 14$	$5 \cdot 2 = 10$
$7 \cdot 3 = 21$	$5 \cdot 3 = 15$
$7 \cdot 4 = 28$	$5 \cdot 4 = 20$
	$5 \cdot 5 = 25$

Fonte: Produção do próprio autor.

$$\ell(7,5) = \begin{cases} 7-5=2, \\ 14-5=9, \\ 14-10=4, \\ 21-5=16, \\ 21-10=11, \\ 21-15=6, \\ 21-20=1, \\ 28-5=23, \\ 28-10=18, \\ 28-15=13, \\ 28-20=8, \\ 28-25=3, \end{cases}$$

Portanto, c é diferente dos elementos do conjunto $\{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\}$ e $7x + 5y = c$ irá admitir solução se $c \notin \ell(7, 5)$.

Exemplo 3.5.10. *Resolver a equação* $7x + 5y = 19$ *em* $N \cup \{0\}$*:*

Usando os dados do Exemplo 3.5.9, a Tabela 11 mostra que o $mdc(7, 5) = 1$ *e com a ajuda do algoritmo de Euclides, será permitido achar a solução particular da equação* x_0, y_0

$$1 = 5 - 2 \cdot 2$$

$$2 = 7 - 5 \cdot 1$$

Substituindo os valores: $mdc(7, 5) = 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5 \cdot 1) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7$

$$1 \cdot (19) = (3 \cdot 5 - 2 \cdot 7) \cdot (19)$$

$$19 = 57 \cdot 5 - 38 \cdot 7$$

conclui-se que $(-38, 57)$ *é uma solução particular da equação e as demais podem ser escritas na forma:*

$$x = -38 + 5t \ \ e \ \ y = 57 - 7t \tag{3.14}$$

De acordo com enunciado, os pares de soluções podem ser apenas não negativos, então tem-se $x \geq 0$ *e* $y \geq 0$.

$$\begin{array}{c|c} x = -38 + 5t & y = 57 - 7t \\ x \geq 0 & y \geq 0 \\ -38 + 5t \geq 0 & 57 - 7t \geq 0 \\ t \geq \dfrac{38}{5} & t \leq \dfrac{57}{7} \end{array}$$

com $t \in \mathbb{Z}$. *Portanto,* $7{,}6 \leq t \leq 8{,}14 \Rightarrow t = 8$

Logo a equação terá solução única em $N \cup \{0\}$, *com* $x = -38 + 5 \cdot 8 = 2$ *e* $y = 57 - 7 \cdot 8 = 1$

3.6 Congruência modular

A congruência modular tem sua origem nas civilizações antigas. Foram os chineses que apresentaram métodos para solucionar sistemas de restos, chegando no conhecido Teorema Chinês do Resto, documentado no século III d.C., mas foi formalizada por Carl Friedrich Gauss, no século XIX. Seu progresso está ligado ao aperfeiçoamento da teoria dos números e à necessidade de entender sobre a aritmética dos inteiros.

Segundo APOSTOL (APOSTOL, 1976), a congruência modular representa a ligação entre inteiros em termos de divisibilidade. A divisão com resto diferente de zero é estudada no Ensino Fundamental II e Médio como uma maneira de apresentar o conceito de congruência modular. Isso simplifica o entendimento dos estudantes, porque relaciona o assunto abstrato da congruência com algo que já conhecem: a divisão Euclidiana.

No Ensino Fundamental, os alunos aprendem que qualquer número a pode ser escrito na forma da divisão por um número n, sendo $a, n \in \mathbb{Z}$

$$a = nq + b, \tag{3.15}$$

onde

- q é o quociente da divisão de a por n;
- b é o resto da divisão com $0 \leq b < n$.

Em outras palavras, é permitido dizer que a é congruente a b módulo n, quando os restos das divisões de a e b por n forem iguais. De forma que na linguagem matemática fica:

$$a \equiv b \mod n \tag{3.16}$$

Propriedades: $\forall n \in \mathbb{N}, \quad \forall a, b, c \in \mathbb{Z}$:

1. $a \equiv a \mod n$;
2. $a \equiv b \mod n$, então $b \equiv a \mod n$;
3. $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$.

Exemplo 3.6.1. *Alguns exemplos de congruência de acordo com as propriedades:*

1. $11 \equiv 11 \mod 10$;
2. $11 \equiv 1 \mod 10$, *então* $1 \equiv 11 \mod 10$;
3. $11 \equiv 1 \mod 10$ *e* $1 \equiv 21 \mod 10$, *então* $11 \equiv 21 \mod 10$.

Proposição 3.6.2. *Supondo que* $a, b, n \in \mathbb{Z}$, *com* $n > 1$, *então* $a \equiv b \mod n$ *se, e somente se,* $n|(a - b)$.

Demonstração:

Ida: Suponha que $a \equiv b \mod n$. Isso significa, por definição de congruência modular, que existe um inteiro k tal que:

$$a - b = k \cdot n.$$

Assim, concluímos que n divide $(a - b)$, ou seja, $n|(a - b)$.

Volta: Suponha agora que $n|(a - b)$. Isso significa que existe um inteiro k tal que:

$$a - b = k \cdot n.$$

Pela definição de congruência, essa equação é equivalente a dizer que:

$a \equiv b \mod n$.

Portanto, foi provado que $a \equiv b \mod n$ se, e somente se, $n|(a - b)$.

Proposição 3.6.3. ***Operação de adição:*** *considerando* $a, b, c, d, n \in \mathbb{Z}$ *e sendo* $n > 1$. *Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$, *então* $a + c \equiv b + d \mod n$

Demonstração: Supondo, por hipótese, que $a \equiv b \mod n \Rightarrow n|(a-b)$ e $c \equiv d \mod n \Rightarrow n|(c-d)$. Logo, $n|(a-b)+(c-d)$ e com o pensamento análogo, é possível usar a operação de subtração $n|(a-b)-(c-d)$. Provando assim, que $a+c \equiv b+d \mod n$ quando $a \equiv b \mod n$ e $c \equiv d \mod n$.

Exemplo 3.6.4. *Aqui segue um exemplo da Proposição 3.6.3, de adição:* $12 \equiv 5 \mod 7$ *e* $20 \equiv 6 \mod 7$, *então* $12 + 20 \equiv 5 + 6 \mod 7 \Rightarrow 32 \equiv 11 \equiv 4 \mod 7$.

Em alguns casos será necessário aplicar o conceito de **inverso aditivo** de um número a módulo n que pode ser definido da seguinte maneira: um número b é o oposto de a módulo n quando $a + b \equiv 0 \mod n$. A Tabela 13 mostra exemplos de adição no contexto da aritmética modular, especificamente módulo 7.

Tabela 13 – Operação de adição módulo 7.

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Fonte: Produção do próprio autor.

Observando o número destacado em vermelho na tabela: A congruência $6 + 5 = 11 \equiv 4 \mod 7$ significa que a diferença entre 11 e 4 é um múltiplo de 7. De fato, $11 - 4 = 7$ e 7 é um múltiplo de 7 (pois $7 = 7 \times 1$). Por isso,

$$11 \equiv 4 \mod 7$$

Propriedades do Inverso Aditivo

1. **Único para cada número módulo** n: O inverso aditivo de um número a módulo n é único, pois a equação $a + b \equiv 0 \mod n$ tem uma única solução para b dentro do conjunto $\{0, 1, ..., n-1\}$.

2. **Se** $a \equiv b \mod n$**, então seus inversos também são congruentes**: $-a \equiv -b \pmod{n}$.

3. **O inverso aditivo de um número pode ser encontrado subtraindo-o de** n: $b = n - a$. Isso funciona porque $a + (n - a) = n \equiv 0 \mod n$

Classes de Resíduos módulo n

Na aritmética modular, a **classe de resíduos módulo** n de um número inteiro a é o conjunto de todos os inteiros que deixam resto na divisão euclidiana por n igual ao resto da divisão de a por n. Ou seja, é o conjunto de números que deixam o mesmo resto quando divididos por n.

Matematicamente, a classe de resíduos de a módulo n é representada como $[a]_n = \{x \in \mathbb{Z} \,|\, x \equiv a \mod n\}$. Isso significa que qualquer número x pertencente a $[a]_n$ satisfaz a relação:

$$x = a + k \cdot n, \text{para algum } k \in \mathbb{Z}. \tag{3.17}$$

Exemplo 3.6.5. *Para* $n = 7$*, existem exatamente* 7 ***classes de resíduos****, pois qualquer número inteiro é congruente a um dos valores* $0, 1, 2, 3, 4, 5, 6$ *módulo* 7 *.*

As classes de resíduos são:

$[0]_7 = \{..., -14, -7, 0, 7, 14, 21, \cdots\}$

$[1]_7 = \{..., -13, -6, 1, 8, 15, 22, \cdots\}$

$[2]_7 = \{..., -12, -5, 2, 9, 16, 23, \cdots\}$

$[3]_7 = \{..., -11, -4, 3, 10, 17, 24, \cdots\}$

$[4]_7 = \{..., -10, -3, 4, 11, 18, 25, \cdots\}$

$[5]_7 = \{..., -9, -2, 5, 12, 19, 26, \cdots\}$

$[6]_7 = \{..., -8, -1, 6, 13, 20, 27, \cdots\}$

Cada número inteiro pertence a exatamente uma dessas classes. Assim, ao trabalhar com aritmética modular, podemos ***representar qualquer número inteiro*** *por um único representante da sua classe de resíduo.*

Propriedade Importante:

O conjunto de todas as classes de resíduos módulo n forma o **conjunto dos restos módulo** n:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\} \tag{3.18}$$

Isso significa que, em aritmética modular, qualquer número inteiro pode ser substituído pelo seu representante na classe de resíduos correspondente.

Exemplo 3.6.6.

- 11 *pertence à classe* $[4]_7$ *porque* $11 \div 7$ *tem resto* 4*, então:*

$$11 \equiv 4 \mod 7$$

- 23 *pertence à classe* $[2]_7$ *porque* $23 \div 7$ *tem resto* 2*, então:*

$$23 \equiv 2 \mod 7$$

As classes de resíduos são fundamentais na teoria dos números e na criptografia, porque permite que seja trabalhado apenas com um conjunto reduzido de números, ignorando múltiplos de n. Isso simplifica cálculos e possibilita aplicações como a **criptografia modular** e teoria dos grupos.

Proposição 3.6.7. ***Operação de multiplicação:*** *considerando* $a, b, c, d, n \in \mathbb{Z}$ *e sendo* $n > 1$*. Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$*, então* $a \cdot c \equiv b \cdot d \mod n$

Demonstração: Supondo, por hipótese, que $a \equiv b \mod n \Rightarrow n \cdot k_1 = (a - b)$ e $c \equiv d \mod n \Rightarrow n \cdot k_2 = (c - d)$, sendo $k_1, k_2 \in \mathbb{Z}$. Se as duas equações implicadas forem multiplicadas, será encontrado: $(a - b) \cdot (c - d) = (n \cdot k_1)(n \cdot k_2) \Rightarrow ac - ad - bc + bd + ad + bc - 2bd = k_1 \cdot k_2 \cdot n^2 + ad + bc - 2bd \Rightarrow ac - bd = ad - bd + bc - bd + k_1 \cdot k_2 \cdot n^2 \Rightarrow ac - bd = (a - b)d + (c - d)b + (k_1 \cdot k_2 \cdot n^2)$. Substituindo as igualdades $(a - b) = n \cdot k_1$ e $(c - d) = n \cdot k_2$ será identificado que $a \cdot c - b \cdot d = (n \cdot k_1)d + (n \cdot k_2)b + (k_1 \cdot k_2 \cdot n^2)$. Sendo assim, se $n|(ac - bd)$ então $a \cdot c \equiv b \cdot d \mod n$.

Exemplo 3.6.8. *Aqui segue um exemplo da Proposição 3.6.7, de multiplicação:* $8 \equiv 2 \mod 3$ *e* $10 \equiv 1 \mod 3$*, então* $8 \cdot 10 \equiv 2 \cdot 1 \mod 3 \Rightarrow 80 \equiv 2 \mod 3$.

Proposição 3.6.9. ***Operação de potenciação:*** *Considerando* $\forall n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$*. Se* $a \equiv b \mod n$*, então* $a^n \equiv b^n \mod n$

Demonstração: Provando por indução em n:

i. Base da indução: Quando $n = 1$, $a^1 = a \equiv b = b^1 \mod n$,

   A sentença é válida!

ii. Passo indutivo: Supondo que se $p(n)$ é válido, então $n+1$:

Por hipótese, $a^n \equiv b^n \mod n$ é verdade, mas faz-se necessário mostrar que também é verdade $a^{n+1} \equiv b^{n+1} \mod n$.

Considerando que $a^{n+1} = a^n \cdot a$ e $b^{n+1} = b^n \cdot b$. Então, a multiplicação das congruências $a^n \equiv b^n \mod n$ e $a \equiv b \mod n$ implica em $a^n \cdot a \equiv b^n \cdot b \mod n$ e por transitividade, a equação modular fica $a^{n+1} \equiv b^{n+1} \mod n$.

Já foi demonstrado, na Proposição 3.6.7, operações de multiplicação em equações modulares.

Portanto, pelo princípio da indução matemática, $a^{n+1} \equiv b^{n+1} \mod n, \forall n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$.

Exemplo 3.6.10. *Aqui segue um exemplo da Proposição 3.6.9, de potenciação:* $10 \equiv 1 \mod 9$ *então* $10^4 \equiv 1^4 \mod 9$, *então* $10000 \equiv 1 \mod 9$.

Proposição 3.6.11. *Considerando* $a, b, c \in \mathbb{Z}$ *e* $n \in \mathbb{N}$, *se* $(a+b) \equiv (a+c) \mod n$ *então* $b \equiv c \mod n$.

Demonstração: Por hipótese, $(a+b) \equiv (a+c) \mod n$ e pela definição de congruência, isso significa que existe um inteiro k tal que: $(a+b) - (a+c) = k \cdot n \Rightarrow a + b - a - c = k \cdot n \Rightarrow b - c = k \cdot n$. Portanto, é possível concluir que $b \equiv c \mod n$

Exemplo 3.6.12. *Se* $(3+7) \equiv (3+1) \mod 6 \Rightarrow 10 \equiv 4 \mod 6$, *então* $7 \equiv 1 \mod 6$.

Proposição 3.6.13. *Considerando* $a, b, c \in \mathbb{Z}$ *e* $n \in \mathbb{N}$, *se* $(a \cdot b) \equiv (a \cdot c) \mod n$ *e se* a *e* n *forem coprimos, então* $b \equiv c \mod n$.

Demonstração: Por hipótese, $(a \cdot b) \equiv (a \cdot c) \mod n$ e pela definição de congruência, isso significa que: Como $n|(ab - ac)$, ou seja, $n|(a(b-c))$ e a e n são coprimos, então, pelo Lema 3.3.2, de Gauss, segue que $n|(b-c)$ e, portanto, $b \equiv c \mod n$.

Exemplo 3.6.14. *Para ilustrar a proposição 3.6.13, considere* $a = 11$, $b = 4$, $c = 1$ *e* $n = 3$. *Note que* $a = 11$ *e* $n = 3$ *são coprimos.*

Se $(11 \cdot 4) \equiv (11 \cdot 1) \mod 3 \Rightarrow 44 \equiv 11 \equiv 2 \mod 3$. *Como a hipótese da proposição é satisfeita, ou seja,* $a \cdot b \equiv a \cdot c \mod n$ *e* $mdc(a, n) = 1$. *Então, pelo resultado demonstrado, podemos concluir que* $4 \equiv 1 \mod 3$.

3.7 Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat é fundamental na teoria dos números, sendo amplamente usado em algoritmos de criptografia de chave pública, como o RSA. Pierre de

Fermat, matemático nascido no século $XVII$, conseguiu generalizar um resultado que os chineses haviam constatado antes mesmo do início da Era Cristã começar: $p|(2^p-2)$, sendo p um número primo qualquer. Essa congruência ajudou Fermat a formular a propriedade $p|(a^p-a)$, estabelecendo um dos teoremas mais importantes da aritmética modular.

Lema 3.7.1. *Se p é um número primo, então todos os números $\binom{p}{i}$, com $0 < i < p$, são divisíveis por p.*

Demonstração: Tome que $\binom{p}{i} = \dfrac{p!}{i! \cdot (p-i)!}$, sendo $i \in \mathbb{N}$.

Sabendo que o numerador é $p!$, o valor pode ser substituído por $p \cdot (p-1) \cdots 3 \cdot 2 \cdot 1$ e o denominador $i!$ por $i \cdot (i-1) \cdots 3 \cdot 2 \cdot 1$ e $(p-i)!$ por $(p-i) \cdot (p-i-1) \cdots 3 \cdot 2 \cdot 1$.

No numerador $p!$, o número p aparece como maior fator. Já no denominador, o número i, que por hipótese é menor que p, aparece como maior fator de $i!$, o número $(p-i)$, que é menor que p, pois $0 < i$, aparece como maior fator de $(p-i)!$ e como p é primo, nenhuma multiplicação no denominador terá p como produto. Portanto, não se tem o fator p no denominador, significando assim que $p|\binom{p}{i}$ uma vez que p aparece no numerador de $\binom{p}{i}$.

Teorema 3.7.2. ***Pequeno Teorema de Fermat***

Se p é um número primo, então $p|(a^p-a)$, para todo $a \in \mathbb{Z}$

Demonstração: Por indução

i. Base da indução

   Para $a = 0$

$$p|(0^p - 0)$$
$$p|0$$

   Logo a sentença é válida!

ii. Hipótese de indução

   Supondo que $p(a) : p|(a^p-a)$ seja verdade, então $p|((a+1)^p-(a+1))$?

   Expandindo $(a+1)^p$:

$$(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^i.$$

   Agora, analisamos essa soma $\pmod p$. Pelo Lema 3.7.1, sabemos que para $0 < i < p$, os coeficientes binomiais $\binom{p}{i}$ são divisíveis por p, ou seja,

$$\binom{p}{i} \equiv 0 \pmod p,\ 0 < i < p.$$

Desta forma, o lema ajuda a demonstrar o teorema. De fato, o que está em vermelho na equação a seguir é divisível por p. Já os extremos, que estão em preto, são divisíveis por p por hipótese.

$$(a+1)^p - (a+1) = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a^1 + \binom{p}{p}a^0 - (a+1).$$

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a^1 - a$$

Portanto, pelo princípio da indução matemática, o teorema é válido para todo a inteiro.

Corolário 3.7.3. *Se p é primo, e se a é um natural não é múltiplo de p, então $p|(a^{p-1}-1)$:*

Demonstração: Pelo Pequeno Teorema de Fermat (Teorema 3.7.2) p divide $a^p - a = a \cdot (a^{p-1} - 1)$. Como, por hipótese $p \nmid a$, então necessariamente $p \mid (a^{p-1} - 1)$.

O exemplo a seguir é uma aplicação do Pequeno Teorema de Fermat e do Corolário 3.7 à solução de um problema:

Exemplo 3.7.4. *Achar o resto da divisão de 12^{p-1} por p quando p é um número primo:*

Solução: *Pelo Pequeno Teorema de Fermat, $p|(12^p - 12) = 12 \cdot (12^{p-1} - 1)$.*

1. *Se $p \notin \{2, 3\}$, seguramente, $p \nmid 12$. Logo, pode-se dizer que $p|(12^{p-1} - 1)$, já que o $mdc(12, p) = 1$. Assim,*

$$12^{p-1} \equiv 1 \mod p, \text{ portanto } resto_1 = 1$$

2. *Se $p \in \{2, 3\}$, é trivial dizer que $p|12$. Portanto $resto_2 = 0$*

Exemplo 3.7.5. *Mostrar que $20|(a^5 - a)$ para qualquer a ímpar, sendo $mdc(a, 5) = 1$*

Solução: *Basta mostrar que $4|(a^5 - a)$ e $5|(a^5 - a)$, porque $4 \cdot 5 = 20$, porém já foi demonstrado no Teorema 3.7.2, o Pequeno Teorema de Fermat, que $5|(a^5 - a)$.*

Assim, $a^5 - a = a(a^4 - 1) = a \cdot (a^2 - 1) \cdot (a^2 + 1) = a \cdot (a - 1) \cdot (a + 1) \cdot (a^2 + 1)$

1. *Como, por hipótese, a é ímpar, ele pode ser escrito da forma $2k - 1$, então $a + 1$ e $a - 1$ são pares. Logo, a multiplicação entre esses dois pares resulta num número múltiplo de 4:*

$$a \cdot (a-1) \cdot (a+1) = (2k-1) \cdot [(2k-1) - 1] \cdot [(2k-1) + 1] = (2k-1) \cdot 2(k-1) \cdot 2k = (2k-1) \cdot 4k(k-1)$$

Isso garante que $4|(a \cdot (a-1) \cdot (a+1) \cdot (a^2+1)) = a^5 - a$.

Portanto, $4 \cdot 5 = 20|(a^5 - a)$ *quando a for ímpar, como era para ser demonstrado.*

Escrever o Pequeno Teorema de Fermat na forma de congruência modular: $a^p \equiv a \mod p$, sendo p primo, $a \in \mathbb{Z}$ e $mdc(a,p) = 1$. Simplificando a equação modular, tem-se que $a^{p-1} \equiv 1 \mod p$.

Exemplo 3.7.6. *Calcular o resto da divisão* 23^{28} *por* 7*:*

Solução: *Note que* $23^{28} = (23^6)^4 \cdot 23^4 \equiv (1)^4 \cdot 23^4 \mod 7$ *pelo Pequeno Teorema de Fermat. Então,* $23^{28} \equiv 1 \cdot 23^4 \mod 7 \Rightarrow 23^{28} \equiv 23^4 \mod 7$. *Além disso, reduzindo:* $23 \equiv 2 \mod 7 \Rightarrow 23^4 \equiv 2^4 \equiv 16 \equiv 2 \mod 7$. *Então, por transitividade,* $23^{28} \equiv 2 \mod 7$. *Portanto, o resto da divisão é* 2.

3.8 Euler

Leonhard Euler, Suíço nascido em 1707, foi um renomado matemático (Figura 9). Segundo Hefez (HEFEZ, 2014), Euler produziu muito material sobre matemática ao logo de sua jornada acadêmica, mesmo com a perda da visão, ele só parou de realizar seus feitos científicos com sua morte, em 1783.

Figura 9 – Euler.

Fonte: Disponível em: <https://www3.unicentro.br/petfisica/2016/06/29/leonhard-euler-1707-1783/> . Acesso em 29/01/2025

O trabalho de Euler continua sendo importante, ainda nos dias atuais, na criptografia moderna, especialmente por suas colaboração à teoria dos números. Diversos conceitos que ele descreveu são fundamentais para sistemas de criptografia usados na contemporaneidade, como o RSA. Aqui estão algumas das principais influências dele na criptografia:

3.8.1 Números Primos e Fatoração:

Euler pesquisou sobre os números primos, um tema importantíssimo na criptografia. O fato de ser muito trabalhoso fatorar números muito grandes, produto de dois primos grandes, é o que promete a proteção de métodos como o RSA.

Ainda que Euler não tenha trabalhado de modo direto com criptografia, que só foi se tornar uma ciência moderna no século XX, as ideias de Euler compõem a base da matemática dos sistemas usados atualmente. Sem seus auxílios, o RSA e outros métodos assimétricos não existiriam no formato como conhecemos.

3.8.2 Função Totiente de Euler

A função Totiente de Euler, definida como $\varphi(n)$ conta qual a quantidade de números inteiros de 1 até n são relativamente primos com $n-1$, ou melhor dizendo, mdc entre eles é igual a 1. No RSA, essa função é um componente muito importante, porque se baseia no fato de que contar $\varphi(n)$ é simples se a fatoração de n for conhecida, mas custoso caso n seja um número muito grande composto de dois primos desconhecidos.

Teorema 3.8.1. *Se $p \geq 2$, sendo p um número primo, então $\varphi(p) = p - 1$*

Demonstração: Como, por hipótese, p é primo, então todos os números menores que ele não dividem p. Portanto, p tem uma quantidade de $p-1$ primos relativos a ele no conjunto $\{1, 2, \ldots, p-1\}$.

Exemplo 3.8.2. *$\varphi(7) = 7 - 1 = 6$, pois $mdc(1,7) = mdc(2,7) = mdc(3,7) = mdc(4,7) = mdc(5,7) = mdc(6,7) = 1$.*

Teorema 3.8.3. *Se p e q são números primos, então*

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) = p \cdot q - p - q + 1. \tag{3.19}$$

Demonstração: Considere:

1. os números inteiros menores que $p \cdot q$ são $\{1, 2, \cdots, pq-1\}$
2. um número x qualquer nesse intervalo é relativamente primo com pq, ou seja, $mdc(x, pq) = 1$, se, e somente se, não for divisível por p nem por q.
3. É necessário contar os números que não são divisíveis por p ou q:

- O total de números de 1 a $pq-1$ é $pq-1$.
- Os números divisíveis por p são $\{p, 2p, 3p, ..., (q-1)p\}$, que são $q-1$ números.

- Os números divisíveis por q são $\{q, 2q, 3q, ..., (p-1)q\}$, que são $p-1$ números.
- Os números divisíveis por ambos (múltiplos de pq) são apenas 0 e pq, então não precisam ser subtraídos.

Assim, o número de inteiros menores que pq que não são divisíveis por p nem por q é:

$$p \cdot q - 1 - (q-1) - (p-1) = p \cdot q - p - q + 1.$$

Portanto, foi demonstrado que $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$.

Exemplo 3.8.4. *Note que* $\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = (2-1) \cdot (7-1) = 1 \cdot 6 = 6$, *pois* $mdc(14,1) = mdc(14,3) = mdc(14,5) = mdc(14,9) = mdc(14,11) = mdc(14,13) = 1$ *e* $mdc(14,2), mdc(14,4), mdc(14,6), mdc(14,7), mdc(14,8), mdc(14,10), mdc(14,12) \neq 1$.

Lema 3.8.5. *Se p é um número primo e $r \in \mathbb{N}$, então*

$$\varphi(p^r) = p^r - p^{r-1} = p^r \cdot \left(1 - \frac{1}{p}\right) \tag{3.20}$$

Demonstração: A quantidade total de números de 1 até p^r é p^r. Para calcular $\varphi(p^r)$ deve-se subtrair desse total a quantidade de múltiplos de p. Esses múltiplos formam o conjunto $M(p) = \{p, 2p, \cdots p^{r-1} \cdot p\}$, o qual contém p^{r-1} elementos. Portanto, como foi demonstrado, $\varphi(p^r) = p^r - p^{r-1} = p^r \cdot \left(1 - \frac{1}{p}\right)$.

Exemplo 3.8.6. *Para determinar* $\varphi(16)$, *deve-se considerá-lo de forma fatorada,* $16 = 2^4$. *A quantidade de números que tem de* 1 *até* 16 *é* 16 *e o conjunto que representa os múltiplos de* 2 *é* $M(2) = \{2, 4, 6, 8, 10, 12, 14, 16\}$, *isto é, um conjunto de* 8 *elementos ou* 2^3 *elementos. Portanto* $\varphi(16) = 2^4 - 2^3 = 16 - 8 = 8$.

Teorema 3.8.7. *Se m e n são números positivos primos entre si, então*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Demonstração: A demonstração deste teorema pode ser encontrada em (HEFEZ, 2014).

Teorema 3.8.8. *Seja $n > 1$ e $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ a sua a forma fatorada, sendo para algum $m \in \mathbb{N}$, então*

$$\varphi(n) = p_1^{\alpha_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \cdots \cdot p_m^{\alpha_m} \cdot \left(1 - \frac{1}{p_m}\right). \tag{3.21}$$

Demonstração: A demonstração deste teorema sucede do lema anterior (Lema 3.8.5) e do Teorema 3.8.3. A fórmula pode ser reescrita da seguinte maneira:

$$\varphi(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) = p_1^{\alpha_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdots p_m^{\alpha_m} \cdot \left(1 - \frac{1}{p_m}\right). \tag{3.22}$$

Exemplo 3.8.9. *Para determinar* $\varphi(100)$*, deve-se reescrevê-lo na forma fatorada,* $100 = 2^2 \cdot 5^2$.

1. *A quantidade de números que tem de* 1 *até* 2^2 *é* 4 *e o conjunto que representa os múltiplos de* 2 *é* $M(2) = \{2, 4\}$*, isto é, um conjunto de* 2 *elementos ou* 2^1 *elementos.*

$$\varphi(2^2) = 2^2 - 2^1 = 4 - 2 = 2$$

2. *A quantidade de números que tem de* 1 *até* 5^2 *é* 25 *e o conjunto que representa os múltiplos de* 5 *é* $M(5) = \{5, 10, 15, 20, 25\}$*, isto é, um conjunto de* 5 *elementos ou* 5^1 *elementos.*

$$\varphi(5^2) = 5^2 - 5^1 = 25 - 5 = 20$$

Portanto, $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 2 \cdot 20 = 40$

Teorema 3.8.10. ***Teorema de Euler***

Considerando $n, a \in \mathbb{Z}$*, se* $n > 1$ *e* $mdc(a, n) = 1$*, então* $a^{\varphi(n)} \equiv 1 \mod n$.

Demonstração: A demonstração deste teorema pode ser encontrada em (HEFEZ, 2014).

O teorema de Euler é uma generalização do Pequeno Teorema de Fermat, demonstrado no Teorema 3.7.2, porque $a^{\varphi(n)} \equiv 1 \mod n$ pode ser escrito na forma $n|(a^{\varphi(n)} - 1)$, onde φ é a função Totiente de Euler, e $\varphi(p) = p - 1$ quando p é primo como demonstrado no Teorema 3.8.1.

3.9 Congruência Linear

Uma congruência linear é uma equação da forma:

$$ax \equiv b \mod n, \tag{3.23}$$

onde $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e o objetivo é encontrar valores inteiros para x.

Proposição 3.9.1. *A congruência* $aX \equiv b \mod n$*, com* $a, b, n \in \mathbb{Z}$ *e* $n > 1$*, tem solução se, e somente se,* $mdc(a, n)|b$.

Demonstração:

Ida: Supondo, por hipótese, que a congruência $aX \equiv b \mod n$ admite uma solução $X_0 \in \mathbb{Z}$. Então, existe um inteiro k tal que $aX_0 = b + k \cdot n \Rightarrow aX_0 - k \cdot n = b$.

Considerando o $d = mdc(a, n)$, tem-se que d divide tanto $a \cdot X_0$ quanto $k \cdot n$ e por consequência d divide $aX_0 - k \cdot n = b$. Logo, $d|b$.

Volta: Supondo agora, por hipótese, que $d|b$ e a congruência modular seja escrita na forma de equação diofantina, $aX - k \cdot n = b$, então a equação possui solução, porque $d|b$ e é trivial dizer que $d|aX - k \cdot n$.

Exemplo 3.9.2. *Encontrar os possíveis valores de x na congruência:* $3x \equiv 6 \mod 9$

Solução:

- *O* $mdc(3, 9) = 3$. *Como* 3 *divide* 6, *a congruência tem solução.*
- *Assim, a solução geral é:*

$$3x \equiv 6 \mod 9 \Rightarrow 3x = 6 + 9k, k \in \mathbb{Z}$$
$$\Rightarrow x = 2 + 3k, k \in \mathbb{Z}$$

Portanto, qualquer número da forma $2 + 3k$ *é uma solução da congruência.*

Teorema 3.9.3. *Considere a congruência* $aX \equiv b \mod n$, *com* $a, b, n \in \mathbb{Z}$, *com* $n > 1$ *e* $d = mdc(a, n)$. *Se* x_0 *é uma solução desta congruência, então*

$$x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \cdots, x_0 + (d-1) \cdot \frac{n}{d} \tag{3.24}$$

são soluções módulo n *da congruência.*

Demonstração: Sabendo que x_0 é uma solução de $aX \equiv b \mod n$, ou seja, existe um inteiro k tal que $a \cdot x_0 = b + k \cdot n$. Seja j qualquer um dos números $0, 1, \ldots, d-1$, isso significa que os candidatos à solução da congruência podem ser representadas por $x_j = x_0 + j \cdot \frac{n}{d}$.

Substituindo x_j na equação modular inicial: $a(x_0 + j \cdot \frac{n}{d}) \equiv b \mod n$

$$\Rightarrow a \cdot x_0 + a \cdot j \cdot \frac{n}{d} \equiv b \mod n.$$

Tem-se, por hipótese, que $ax_0 \equiv b \mod n$ e pela soma de equação modular é possível identificar que a segunda parcela é $a \cdot j \cdot \frac{n}{d} \equiv 0 \mod n$.

É preciso mostrar que o termo $\frac{a \cdot j \cdot n}{d}$ é múltiplo de n. Como $d = mdc(a, n)$, então $d|a$ e o quociente desta divisão pode ser chamada de a_1. Logo, $\frac{a \cdot j \cdot n}{d} = a_1 \cdot j \cdot n$ é múltiplo de n e $x_0 + j \cdot \frac{n}{d}$ são soluções da congruência $aX \equiv b \mod n$.

Portanto, os valores $x_0, x_0 + \frac{n}{d}, x_0 + 2 \cdot \frac{n}{d}, \ldots, x_0 + (d-1) \cdot \frac{n}{d}$ são as soluções módulo n da congruência dada.

Exemplo 3.9.4. *Considere a congruência* $5X \equiv 10 \pmod{25}$.

Solução: $d = mdc(5, 25) = 5$ e $5|10$, logo a congruência tem exatamente $d = 5$ soluções distintas módulo 25.

Desta forma, a solução geral é dada por $5X = 10 + 25k \Rightarrow X = \dfrac{10 + 25k}{5} \Rightarrow X = 2 + 5k$, $k = 0, 1, 2, 3, 4$ e isso representa as cinco soluções distintas módulo 25: $X = 2, 7, 12, 17, 22$

Se k fosse 5, então: $X = 2 + 5 \cdot 5 = 27 \equiv 2 \mod 25$,

O que confirma que as soluções começam a se repetir, garantindo que há exatamente $d = 5$ soluções distintas.

3.9.1 Teorema Chinês do Resto

Teorema 3.9.5. ***Teorema Chinês dos Restos Generalizado:*** *Seja o sistema de congruências:*

$$\begin{cases} X \equiv C_1 \mod m_1 \\ X \equiv C_2 \mod m_2 \\ \quad \vdots \\ X \equiv C_k \mod m_k \end{cases} \tag{3.25}$$

Se os módulos $m_1, m_2, \cdots, m_k$ não são necessariamente coprimos, então existe uma solução única módulo $M = mmc(m_1, m_2, \cdots, m_k)$ se, e somente se, para todo par i, j, vale: $C_i \equiv C_j \mod mmc(m_i, m_j)$, considerando $i, j = 1, \ldots, k$.

Se essa condição for satisfeita, a solução geral pode ser escrita da seguinte maneira:

$$X = M_1 \cdot Y_1 \cdot C_1 + \cdots + M_k \cdot Y_k \cdot C_k + M \cdot t, \text{sendo } t \in \mathbb{Z}, \tag{3.26}$$

onde $M_i = \dfrac{M}{m_i}$ e Y_i é solução da congruência $M_i Y_i \equiv 1 \mod m_i$

Demonstração: A demonstração deste teorema pode ser encontrada em (HEFEZ, 2014).

Exemplo 3.9.6. *Ache o menor número natural que deixa restos $1, 3, 5$ quando dividido por $5, 7, 9$.*

Solução: Tome que

$$\begin{cases} X \equiv 1 \mod 5 \\ X \equiv 3 \mod 7 \\ X \equiv 5 \mod 9 \end{cases}$$

Note que $mdc(5, 7) = mdc(7, 9) = mdc(5, 9) = 1$, $M = mmc(5, 7, 9) = 315$, $M_1 = 7 \cdot 9 = 63, M_2 = 5 \cdot 9 = 45, M_3 = 5 \cdot 7 = 35$

i. $63 \cdot Y_1 \equiv 1 \mod 5$

$63 \cdot Y_1 \equiv 3 \cdot Y_1 \equiv 1 \mod 5$

$3Y_1 - 5q_1 = 1$

	1	1	
5	3	2	1
2	1		

$1 = 3 - 2 \cdot 1$

$2 = 5 - 3 \cdot 1$

$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 3 \cdot 2 - 5$, então $Y_1 = 2$

ii. $45 \cdot Y_2 \equiv 1 \mod 7$

$45 \cdot Y_2 \equiv 3 \cdot Y_2 \equiv 1 \mod 7$

$3Y_2 - 7q_2 = 1$

	2	3
7	3	1
1		

$1 = 7 - 3 \cdot 2$, então $Y_2 = -2 \equiv 5 \mod 7$

iii. $35 \cdot Y_3 \equiv 1 \mod 9$

$35 \cdot Y_3 \equiv 8 \cdot Y_3 \equiv 1 \mod 9$

$8Y_3 - 9q_3 = 1$

	1	8
9	8	1
1		

$1 = 9 - 8 \cdot 1$, então $Y_3 = -1 \equiv 8 \mod 9$

A solução geral dada para um sistema de congruências é

$$X = M_1 \cdot Y_1 \cdot C_1 + M_2 \cdot Y_2 \cdot C_2 + M_3 \cdot Y_3 \cdot C_3 + M \cdot t, \text{sendo } t \in \mathbb{Z} \tag{3.27}$$

$\Rightarrow X = 63 \cdot 2 \cdot 1 + 45 \cdot 5 \cdot 3 + 35 \cdot 8 \cdot 5 + 315 \cdot t$

Para $X \in \mathbb{N}$, temos $X \geq 0$.

$\Rightarrow 63 \cdot 2 \cdot 1 + 45 \cdot 5 \cdot 3 + 35 \cdot 8 \cdot 5 + 315 \cdot t \geq 0 \Rightarrow t \geq -6$.

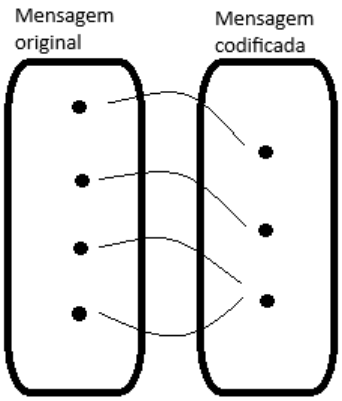
Para que X seja o menor possível devemos ter $t = -6$. Logo, substituindo t na expressão acima, obtemos $X = 311$.

4 O algoritmo da Criptografia RSA

Codificar uma mensagem é pegar um grupo de informações e transformar em um outro conjunto de informações que não possa ser identificada por qualquer pessoa e para que esse processo seja eficiente, ele precisa satisfazer algumas exigências:

- Se as informações são um conjunto de quatro mensagens originais, mas a quarta informação original se transforma na mesma codificação da terceira, como mostra o esquema da Figura 10. Isso é um problema para o método, porque o receptor ao decodificar, não saberá qual é a mensagem original!

Figura 10 – Esquema que traz ambiguidade na informação original.

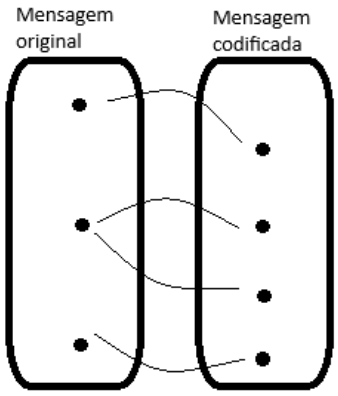


Fonte: Produção do próprio autor.

- Outro preceito relevante da criptografia é que não pode acontecer que uma mensagem original produza duas codificações diferentes, como no esquema da Figura 11. Quando isso ocorre, significa dizer que o sistema criptográfico não é eficaz e a segurança da mensagem pode estar comprometida.

  O propósito é que todo sistema seja reversível, mas apenas para o receptor que possui a chave correta, evitando que haja ambiguidade na hora de decodificar a mensagem. Dois exemplos de unicidade de cifragem são a cifra de Vigenère e a cifra de César, em que uma informação original sempre produz uma única mensagem criptografada.

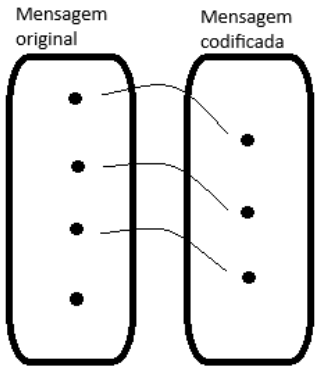
Figura 11 – Esquema que traz uma informação original e duas codificações.



Fonte: Produção do próprio autor.

- Se houver quatro mensagens originais e uma dessas informações não poder ser transformada em uma informação criptografada, como na Figura 12. Isso também será um problema para o método, porque, de fato, a informação será incompleta.

Figura 12 – Esquema que traz codificação com informação incompleta.



Fonte: Produção do próprio autor.

Se o conteúdo de função já foi estudado, pode-se observar que a bijetividade não acontece no esquema da Figura 10 e os esquemas das Figuras 11 e 12 não são considerados funções. Ou seja, para que exista um bom funcionamento de métodos criptográficos o ideal é que o sistema trabalhe de acordo com uma função bijetora.

Se o método de codificação for fácil de ser quebrado, qualquer pessoa pode ter acesso ao conjunto de informações que o mensageiro tentou passar secretamente. E isso também faz com que o sistema criptográfico, na prática, seja ruim ainda que ele trabalhe de forma bijetiva. Por isso, o grande mérito do método RSA é agir de maneira simultânea como função injetiva e sobrejetiva e ser de difícil decodificação.

O algoritmo da criptografia RSA tem como característica efetuar a multiplicação de dois números primos p e q, que são muito grandes, e chamar esse produto de "chave pública":

$$p \cdot q = n \qquad \text{(chave pública)}$$

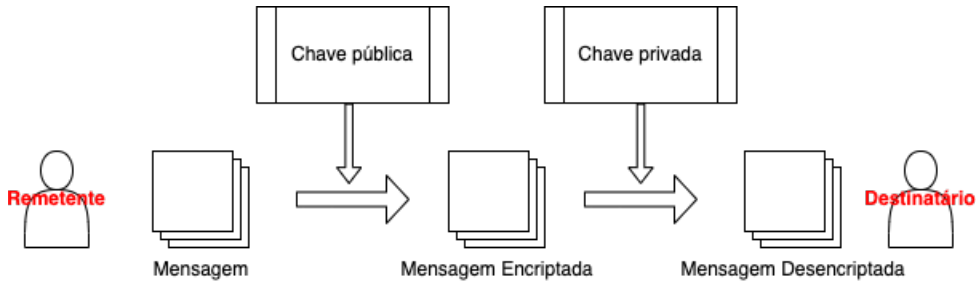
Isso acontece para que a pessoa que conhece a chave pública, não consiga identificar quais são os valores de p e q. Porque não existe uma forma rápida e eficiente para quebrar o número n e descobrir os dois primos para poder decodificar as mensagens.

4.1 Definição de chave assimétrica

A chave assimétrica é uma ideia da criptografia onde se usa um par de chaves diferentes:

1. **Chave pública:** É dada por (λ, n), onde λ é chamado de expoente público. Essa chave pode ser compartilhada livremente e é utilizada para criptografar as mensagens originais.
2. **Chave privada:** É dada por (d, n), onde d é o inverso $\lambda \mod \varphi(n)$ e $\varphi(n) = (p-1) \cdot (q-1)$, devendo ser mantida em segredo é usada para descriptografar as mensagens codificadas com a chave pública.

Figura 13 – Esquema de chave assimétrica.



Fonte: Disponível em: <https://dicionariotec.com/posts/algoritmo-de-chave-assimetrica>. Acesso em 03/03/2025

Esse método é chamado de criptografia de chave pública e ele é diferente da criptografia simétrica, onde a mesma chave é utilizada tanto para codificar quanto para decodificar. A segurança da criptografia de chave pública vem do fato de que, mesmo conhecendo a chave pública, é praticamente impossível calcular a chave privada em um espaço de tempo ideal.

> Uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isto mesmo é chamada como chave pública. Por outro lado, para decifrar mensagens, há a necessidade de uma chave secreta, conhecida apenas pelo indivíduo para o qual a mensagem foi enviada. Por isto, esta chave é conhecida como chave secreta (BEZERRA D. DE J.; MALAGUTTIV, 2010, p. 108).

4.2 Codificação

A Criptografia RSA é um mecanismo de codificação mais avançado e neste capítulo será trabalhado o algoritmo do método. Ou seja, como se criptografa as informações de acordo com RSA.

Antes de codificar qualquer mensagem, é necessário que se passe por uma etapa de pré-codificação, que é associar cada letra da mensagem a um número, de dois algarismos, como no exemplo da Tabela 14.

Tabela 14 – Associação de letra a um número de dois algarismos.

A	10	N	23
B	11	O	24
C	12	P	25
D	13	Q	26
E	14	R	27
F	15	S	28
G	16	T	29
H	17	U	30
I	18	V	31
J	19	W	32
K	20	X	33
L	21	Y	34
M	22	Z	35

Fonte: Produção da própria autora.

Essa codificação é simples, porém eficaz para converter qualquer palavra ou frase em uma sequência numérica, que será então utilizada nas etapas seguintes do algoritmo RSA. Sendo assim, a Tabela 14 é essencial para o início da aplicação prática do RSA.

Mensagem original: PROFMAT

Pré-codificação: 25272415221029

- Para codificar a mensagem original, é indispensável fazer a escolha de dois números primos, p e q, que são os responsáveis por ajudar a criar a chave de codificação.

Se $p = 5$ e $q = 7$, então $n = p \cdot q = 5 \cdot 7 = 35$ (chave de codificação).

- O número da codificação é separado em blocos formando números de qualquer quantidade de algarismos, desde que eles sejam maiores ou iguais a 1 e menores que n: $25 - 27 - 24 - 15 - 22 - 10 - 29$.

Agora, começando a codificação, tome que b é o valor numérico de um bloco. O método impõe que cada b seja elevado a um mesmo natural λ, considerando $\varphi(n) = (p-1)\cdot(q-1)$ o $mdc(\varphi(n), \lambda) = 1$, e determina o resto da divisão do resultado por n, obtendo assim um valor a:

$$b^{\lambda} \equiv a \mod n \tag{4.1}$$

Considerando $\lambda = 7$ e fazendo as contas dos blocos escolhidos anteriormente, tem-se:

1. $25^7 \equiv a \mod 35$

   $25^2 = 625 \Rightarrow 625 \equiv 30 \mod 35$

   $25^4 = (25^2)^2 \equiv 30^2 \equiv 900 \equiv 25 \mod 35$

   $25^7 = 25^4 \times 25^2 \times 25 \equiv 25 \times 30 \times 25 \mod 35$

   $25 \times 30 = 750 \Rightarrow 750 \equiv 15 \mod 35$

   $15 \times 25 = 375 \Rightarrow 375 \equiv 25 \mod 35$

2. $27^7 \equiv a \mod 35$

   $27^2 = 729 \Rightarrow 729 \equiv 29 \mod 35$

   $27^4 = (27^2)^2 \equiv 29^2 \equiv 841 \equiv 1 \mod 35$

   $27^7 = 27^4 \times 27^2 \times 27 \equiv 1 \times 29 \times 27 \mod 35$

   $29 \times 27 = 783 \Rightarrow 783 \equiv 13 \mod 35$

3. $24^7 \equiv a \mod 35$

   $24^2 = 576 \Rightarrow 576 \equiv 16 \mod 35$

   $24^4 = (24^2)^2 \equiv 16^2 \equiv 256 \equiv 11 \mod 35$

   $24^7 = 24^4 \times 24^2 \times 24 = 11 \times 16 \times 24$

   $11 \times 16 = 176 \Rightarrow 176 \equiv 1 \mod 35$

   $1 \times 24 = 24$

4. $15^7 \equiv b \mod 35$

   $15^2 = 225 \Rightarrow 225 \equiv 15 \mod 35$

   $15^4 = (15^2)^2 \equiv 15^2 \equiv 15 \mod 35$

   $15^7 = 15^4 \times 15^2 \times 15 \equiv 15 \times 15 \times 15 \mod 35$

   $15 \times 15 = 225 \Rightarrow 225 \equiv 15 \mod 35$

5. $22^7 \equiv a \mod 35$

   $22^2 = 484 \Rightarrow 484 \equiv 29 \mod 35$

   $22^4 = (22^2)^2 \equiv 29^2 \equiv 841 \equiv 1 \mod 35$

   $22^7 = 22^4 \times 22^2 \times 22 \equiv 1 \times 29 \times 22 \mod 35$

   $29 \times 22 = 638 \Rightarrow 638 \equiv 8 \mod 35$

6. $10^7 \equiv a \mod 35$

   $10^2 = 100 \Rightarrow 100 \equiv 30 \mod 35$

   $10^4 = (10^2)^2 \equiv 30^2 = 900 \equiv 25 \mod 35$

   $10^7 = 10^4 \times 10^2 \times 10 \equiv 25 \times 30 \times 10 \mod 35$

   $25 \times 30 = 750 \Rightarrow 750 \equiv 15 \mod 35$

   $15 \times 10 = 150 \Rightarrow 150 \equiv 10 \mod 35$

7. $29^7 \equiv a \mod 35$

   $29^2 = 841 \Rightarrow 841 \equiv 1 \mod 35$

   $29^4 = (29^2)^2 \equiv 1^2 \equiv 1 \mod 35$

   $29^7 = 29^4 \times 29^2 \times 29 \equiv 1 \times 1 \times 29 \equiv 29 \mod 35$

   Mensagem Codificada: $25 - 13 - 24 - 15 - 8 - 10 - 29$

4.3 Decodificação

Para poder decodificar uma mensagem será preciso ter o conhecimento do valor da chave de decodificação, formada por um par de números. Um deles, já conhecido por n e o outro número é o inverso de $\lambda \mod (p-1)\cdot(q-1)$. Esse número irá aparecer a partir deste momento e será chamado de d. Ou seja,

$$\boxed{\lambda \cdot d \equiv 1 \mod (p-1)\cdot(q-1)}$$

Usando a mensagem original, "PROFMAT" que foi codificada anteriormente, a partir deste momento ela pode ser decodificada: $7 \cdot d \equiv 1 \mod (5-1)\cdot(7-1) \Rightarrow 7 \cdot d \equiv 1 \mod 4 \cdot 6 \Rightarrow 7 \cdot d \equiv 1 \mod 24 \Rightarrow 7d - 24q = 1$. O $mdc(7, 24) = 1$, logo

	3	2	3
24	7	3	$1 = mdc(7, 24)$
3	1	0	

$1 = 7 - 3 \cdot 2$

$3 = 24 - 7 \cdot 3$

$1 = 7 - 3 \cdot 2 = 7 - (24 - 7 \cdot 3) \cdot 2 = 7 \cdot 7 - 24 \cdot 2$. Portanto, $d = 7$.

Encontrado o valor de d, agora pode ser estabelecida uma regra para decodificar uma mensagem: $a^d \equiv b \mod n$.

A mensagem cifrada foi obtida com os números: $a = \{25, 13, 24, 15, 8, 10, 29\}$ e $n = 35$.

1. $25^7 \equiv b \mod 35$

   $25^2 = 625 \Rightarrow 625 \equiv 30 \mod 35$

   $25^4 = (25^2)^2 \equiv 30^2 \equiv 900 \equiv 25 \mod 35$

   $25^7 = 25^4 \times 25^2 \times 25 \equiv 25 \times 30 \times 25 \mod 35$

   $25 \times 30 = 750 \Rightarrow 750 \equiv 15 \mod 35$

   $15 \times 25 = 375 \Rightarrow 375 \equiv 25 \mod 35$, que corresponde à letra **P**.

2. $13^7 \equiv b \mod 35$

   $13^2 = 169 \Rightarrow 169 \equiv 29 \mod 35$

   $13^4 = (13^2)^2 \equiv 29^2 \equiv 841 \equiv 1 \mod 35$

   $13^3 \equiv 29 \times 13 \mod 35 \Rightarrow 377 \equiv 27 \mod 35$

   $13^7 = 13^4 \times 13^3 \equiv 1 \times 27 \equiv 27 \mod 35$, que corresponde à letra **R**.

3. $24^7 \equiv b \mod 35$

   $24^2 = 576 \Rightarrow 576 \equiv 16 \mod 35$

   $24^4 = (24^2)^2 \equiv 16^2 \equiv 256 \equiv 11 \mod 35$

   $24^7 = 24^4 \times 24^2 \times 24 = 11 \times 16 \times 24$

   $11 \times 16 = 176 \Rightarrow 176 \equiv 1 \mod 35$

   $1 \times 24 = 24$, que corresponde à letra **O**.

4. $15^7 \equiv b \mod 35$

   $15^2 = 225 \Rightarrow 225 \equiv 15 \mod 35$

   $15^4 = (15^2)^2 \equiv 15^2 \equiv 15 \mod 35$

   $15^7 = 15^4 \times 15^2 \times 15 \equiv 15 \times 15 \times 15 \mod 35$

   $15 \times 15 = 225 \Rightarrow 225 \equiv 15 \mod 35$, que corresponde à letra **F**.

5. $8^7 \equiv b \mod 35$

   $8^2 = 64 \Rightarrow 64 \equiv 29 \mod 35$

   $8^4 = (8^2)^2 \equiv 29^2 \equiv 1 \mod 35$

$8^3 \equiv 8^2 \times 8 \equiv 29 \times 8 \equiv 232 \equiv 22 \mod 35$

$8^7 = 8^4 \times 8^3 \equiv 1 \times 22$, que corresponde à letra **M**.

6. $10^7 \equiv b \mod 35$

   $10^2 = 100 \Rightarrow 100 \equiv 30 \mod 35$

   $10^4 = (10^2)^2 \equiv 30^2 = 900 \equiv 25 \mod 35$

   $10^7 = 10^4 \times 10^2 \times 10 \equiv 25 \times 30 \times 10 \mod 35$

   $25 \times 30 = 750 \Rightarrow 750 \equiv 15 \mod 35$

   $15 \times 10 = 150 \Rightarrow 150 \equiv 10 \mod 35$, que corresponde à letra **A**.

7. $29^7 \equiv b \mod 35$

   $29^2 = 841 \Rightarrow 841 \equiv 1 \mod 35$

   $29^4 = (29^2)^2 \equiv 1^2 \equiv 1 \mod 35$

   $29^7 = 29^4 \times 29^2 \times 29 \equiv 1 \times 1 \times 29 \equiv 29 \mod 35$, que corresponde à letra **T**.

Mensagem Original Decodificada: PROFMAT

4.4 Decodificando a codificação

No sistema RSA a decodificação de uma mensagem cifrada a recupera a mensagem original b corretamente devido à maneira como as chaves pública e privada são matematicamente relacionadas. De fato, para mostrar que a criptografia RSA funciona, basta provar que

$$p|(b^{\lambda d} - b) \text{ e } q|(b^{\lambda d} - b) \tag{4.2}$$

e, portanto, $n = pq = mmc(p, q)$ divide $(b^{\lambda d} - b)$, donde $b^{\lambda d} \equiv b \mod n$. Consequentemente, temos $a^d \equiv (b^{\lambda})^d \equiv b^{\lambda d} \equiv b \mod n$.

1. No caso em que $p \nmid b$, tem-se pelo Pequeno Teorema de Fermat (Teorema 3.7.2) que $b^{p-1} \equiv 1 \mod p$. A chave privada d é construída de forma que d seja o inverso multiplicativo de λ módulo $\varphi(n) = (p-1)(q-1)$:

   $$\lambda \cdot d \equiv 1 \mod (p-1) \cdot (q-1) \Rightarrow \lambda \cdot d = 1 + k \cdot (p-1)(q-1),$$

   onde $k \in \mathbb{Z}$.

   Desse modo, $b^{\lambda d} = b^{1+k\cdot(p-1)(q-1)} \equiv b \cdot b^{(p-1)^{k(q-1)}} \equiv b \cdot 1^{k(q-1)} = b \mod p$.

2. No caso em que $p|b$ temos $b \equiv 0 \mod p \Rightarrow b^{\lambda d} \equiv 0^{\lambda d} = 0 \equiv b \mod p$.

Um raciocínio análogo mostra que $b^{\lambda d} \equiv b \mod q$.

Isso permite que o criptógrafo aplique o Teorema de Euler (Teorema 3.8.10) e conclua que a exponenciação inverte corretamente a codificação no sistema RSA, recuperando a mensagem original.

4.5 Seleção de primos p e q

Por uniformidade do método RSA, o que se faz na prática é que por consenso o valor de λ é igual a 3. A seguir, será descrito como escolher os primos p e q de modo que os números $(p-1)\cdot(q-1)$ e λ sejam coprimos, para que existe a classe inversa do 3 mod $(p-1)\cdot(q-1)$.

Se $p \equiv 5 \mod 6 \Rightarrow p-1 \equiv 5-1 \mod 6 \Rightarrow p-1 \equiv 4 \mod 6$ e se $q \equiv 5 \mod 6 \Rightarrow q-1 \equiv 4 \mod 6$. Logo, $(p-1)\cdot(q-1) \equiv 4\times 4 \equiv 16 \equiv 4 \mod 6$, transformando a equação modular em equação diofantina, tem-se que $(p-1)\cdot(q-1) = 6\cdot k+4 = 6\cdot k+3+1 = 3\cdot(2k+1)+1$ ou

$$(p-1)\cdot(q-1)\cdot(-1) = -3\cdot(2k+1)-1$$

$$(p-1)\cdot(q-1)(-1) = 3\cdot(-2k-1)-1.$$

Assim, $3\cdot(-2k-1) \equiv 1 \mod (p-1)\cdot(q-1)$. Relembrando que $(p-1)\cdot(q-1) = 6\cdot k+4 \Rightarrow (-2k-1) \equiv 4k+3 \mod (6\cdot k+4)$.

$$\boxed{3\cdot(4k+3) \equiv 1 \mod (6\cdot k+4)}$$

Exemplo 4.5.1. *Se $p=5$, então $5 \equiv 5 \mod 6$ e se $q=11$, então $11 \equiv 5 \mod 6$. Por isso, é possível que o k seja descoberto facilmente, porque $(p-1)\cdot(q-1) = (5-1)\cdot(11-1) = 4\cdot 10 = 40$, como $(p-1)\cdot(q-1) = 6\cdot k+4 \Rightarrow 6\cdot k+4 = 40 \Rightarrow k = 6$*

Se $k=6$, então $4k+3 = 4\cdot 6+3 = 27$. Substituindo na equação $3\cdot(4k+3) \equiv 1 \mod (6\cdot k+4) \Rightarrow 3\cdot 27 \equiv 1 \mod 40$. Portanto, $d=27$.

4.6 O motivo da eficiência do RSA

Segundo HEFEZ (HEFEZ, 2014), apesar dos números primos serem estudados há alguns milhares de anos, foi com o método de Criptografia RSA que surgiu a mais importante aplicabilidade deles e hoje, é difícil imaginar a contemporaneidade sem eles. Com o desenvolvimento da teoria dos números, conteúdo da matemática que estuda sobre o conjunto dos números inteiros e, em especial, os números primos.

Todo número composto pode ser escrito como um produto de números primos e essa decomposição é única, como se fosse a identidade do número. Na teoria, fatorar

números é algo simples, mas na prática, quando esses números são enormes, a forma de achar os primos é pela força bruta, um procedimento que pode demorar semanas, meses, talvez até anos para encontrá-los. Ou seja, não existe maneira eficiente para resolver esse problema de forma rápida.

Exemplo 4.6.1. *Para fatorar o número* 899 *é possível apenas usando lápis e papel.*

Para fatorar o número 3.737 *é melhor usar a calculadora.*

Para fatorar o número 121.103 *é melhor usar o computador.*

Se a pessoa responsável por decodificar a mensagem não conseguir fatorar o número composto n, ele também não vai conseguir descobrir o valor dos dois primos p e q. Como efeito dominó, também não vai conseguir descobrir os valores $(p-1)$ e $(q-1)$ e a resolução da equação $\lambda \cdot d \equiv 1 \mod (p-1) \cdot (q-1)$ será inviável.

O código ASCII (American Standart Code for Information Interchange) é uma tabela (Tabela 14) que pré-codifica os caracteres atribuindo números a letras, números a símbolos para que ao realizar essas substituições, o criptógrafo possa obter uma sequência de números que será quebrada em blocos. Cada um desses blocos tem que respeitar a exigência de $1 \leq b < n$, onde n é o produto entre os dois primos p e q e b o valor do bloco.

Figura 14 – Tabela binária do código ASCII.

Binário	Decimal	Hexa	Glifo
0010 0000	32	20	
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

Binário	Decimal	Hexa	Glifo
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binário	Decimal	Hexa	Glifo
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

Fonte: Disponível em: <https://testebinse.blogspot.com/2016/04/blog-post.htm>. Acesso em: 04/03/2025

5 Sequência didática

Esta sequência didática foi preparada como uma proposta pedagógica, com o objetivo de disponibilizar um planejamento estruturado e sensato sobre o estudo da aritmética no Ensino Básico. Embora não tenha sido aplicado de forma prática, o planejamento visa atender às necessidades de aprendizagem dos alunos do 2ª e 3ª série do Ensino Médio, considerando suas características e o contexto da sala de aula de uma instituição pública de ensino.

A criptografia é uma área de aplicação da matemática, envolvendo definições de álgebra, teoria dos números e lógica, sendo um excelente instrumento pedagógico para o ensino de matemática no Ensino Fundamental II e Ensino Médio. Com o crescimento da dependência de aparelhos de comunicação eletrônicos e armazenamento de informações, o entendimento de como proteger dados sigilosos se torna fundamental.

5.1 Projeto com Atividades para Sala de Aula

Ano/Série: 2º e 3º ano do Ensino Médio.

Objetivos: De acordo com as competências gerais da BNCC (BRASIL. Ministério da Educação, 2018), a proposta pedagógica visa:

1. Incentivar o pensamento crítico: estimular os alunos a refletirem sobre a segurança da informação e a proteger dados pessoais;
2. Contextualizar a matemática na realidade em que o estudante vive: apresentar a importância da matemática na criptografia da sociedade moderna, preparando as crianças para as demandas de tecnologias dos dias atuais.
3. Interagir com seus colegas de classe: trabalhar de forma coletiva para solucionar os problemas de forma mais rápida.

Justificativa: A introdução ao algoritmo da criptografia no Ensino Básico é justificada por sua utilidade no cotidiano dos estudantes, já que o uso de aparelhos eletrônicos, redes sociais e comércio eletrônico está cada vez mais presente no dia-a-dia de crianças, jovens, adolescente e adultos. Além do mais, a criptografia proporciona uma excelente oportunidade de interligar a teoria matemática com problemas práticos, permitindo que os estudantes percebam o valor da matemática no contexto real.

Recursos didáticos:

- Quadro branco;
- Pincel;
- Calculadora;

Conteúdos Abordados: Os tópicos propostos levam em consideração que os alunos já tenham conhecimento prévio de Divisão Euclidiana. Para o estudo de criptografia no Ensino Médio, o assunto pode ser tratado de forma que o professor não se refira a divisão Euclidiana como congruência modular:

- **Introdução à Criptografia:** A história da criptografia (ex: cifra de César, cifra de Vigenère), mostrar rapidamente análise de frequência para quebra de cifras simples e as aplicações modernas de criptografia (ex: RSA).
- **O estudo dos restos:**

  Teorema 5.1.1. *Seja a, b e n, números naturais. Se r_a é o resto da divisão a por n, onde $0 \leq r_a < n$ e r_b é o resto da divisão de b por n, onde $0 \leq r_b < n$, então o resto da divisão de $a + b$ por n é igual ao resto da divisão de $r_a + r_b$ por n.*

  Teorema 5.1.2. *Seja a, b e n, números naturais. Se r_a é o resto da divisão a por n e r_b é o resto da divisão de b por n, onde $0 \leq r_a, r_b < n$, então o resto da divisão de $a \cdot b$ por n é igual ao resto da divisão de $r_a \cdot r_b$ por n.*

  Teorema 5.1.3. *Seja a, b e n, números naturais. Se r_a é o resto da divisão a por n, então o resto da divisão de a^b por n é igual ao resto da divisão de r_a^b por n.*

  Compreender como se faz para achar restos de divisões na calculadora (veja o Apêndice A).

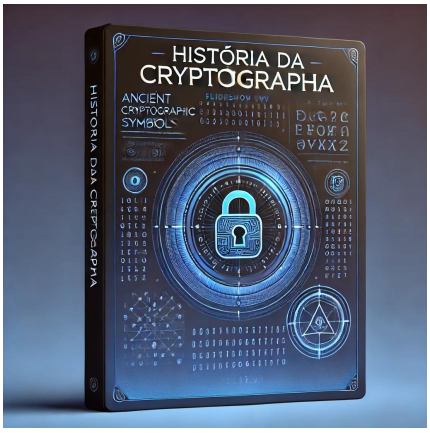
- **Introdução ao RSA**: Função de chave pública e chave privada. Exemplos simples de codificação e decodificação com RSA.

Avaliação: A avaliação será feita de maneira contínua, com ênfase nos conteúdos do projeto elaborado, onde os alunos devem participar da proposta ativamente e mostrar domínio no algoritmo apresentado para codificar e decodificar mensagens curtas.

Desenvolvimento do projeto em sala:

1ª aula
Tempo gasto estimado em uma aula de 50 minutos.
Será a introdução da série de aulas sobre criptografia. Com início na história, os alunos irão embarcar nos fatos com auxílio de slides para uma aula expositiva.

Figura 15 – Capa da série de slides para apresentação da história da criptografia.



Fonte: Gerado pela inteligência artificial do canva.

2ª aula
Tempo gasto estimado em três aulas de 50 minutos cada.
Os alunos poderão assistir o filme que retrata a vida profissional de Alan Turing, o matemático que protagonizou a quebra do código da máquina Enigma durante a 2ª Guerra Mundial.

Figura 16 – Foto de divulgação do filme “O jogo da imitação”.

Fonte: Disponível em: <https://encenasaudemental.com/cinema-tv-e-literatura/alan-turing-e-o-jogo-da-imitacao-o-que-significa-ser-humano/>. Acesso em: 09/03/2025.

5ª aula	Tempo gasto estimado em três aulas de 50 minutos cada.
A aula será introduzida com uma reflexão da responsabilidade ética no uso das redes sociais. No ambiente digital, as ações têm repercussões reais. Ao acessar determinados conteúdos, é feito escolhas que envolvem valores éticos de responsabilidade social. A ética digital envolve o respeito à vida particular de terceiros. Ensinar sobre segurança digital sem considerar a ética seria incompleto. Por isso, é essencial discutir com os alunos os limites entre o que é possível fazer e o que é certo fazer na Internet. Exemplos como o uso indevido de dados sendo apresentados na Internet mostram como a falta de ética pode causar danos graves a outras pessoas. Compreender o funcionamento da criptografia e das boas práticas de segurança digital contribui não só para a proteção individual, mas para a construção de um ambiente virtual mais justo e seguro para todos. Os estudantes do Ensino Médio irão estudar o conteúdo de aritmética dos restos como pré-requisito para o estudo da criptografia RSA. Com pincel de quadro, quadro branco, papel, caneta e calculadora, os alunos irão aprender técnicas de calcular restos de números muito grandes.	
Assunto: Apresentar os Teoremas 5.1.1, 5.1.2 e 5.1.3 e pedir a solução de problemas propostos sobre o assunto.	

Tabela 15 – Problemas propostos para a turma-aula 5 - Lista 1.

Atividades:

1. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de $4633 + 9349$ por 10?
2. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de $9349 - 4633$ por 10?
3. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de 4633×9349 por 10?
4. Ache o resto da divisão de 2^{100} por 11:
5. Ache o resto da divisão $12^{16} + 2^{100}$ por 11:
6. Com auxílio de uma calculadora, ache o resto da divisão de 18423 por 37

Fonte: Produção da própria autora.

A solução da Lista 1 está disponível no Apêndice A.

8ª aula
Tempo gasto estimado em duas aulas de 50 minutos cada.
O tema central do RSA será introduzido com um exemplo que pode ser uma discussão sobre a importância da criptografia na vida cotidiana dos alunos, como a proteção de senhas em redes sociais. Um usuário, quando cria uma senha, ela é transformada em um número e codificada usando a chave pública do servidor. Mesmo que um hacker intercepte a transmissão, ele não conseguirá decodificar a senha do usuário por conta da codificação. Outro exemplo que pode ser dialogado com os alunos é um cenário em que eles desejam realizar uma compra online usando o cartão de seus responsáveis. O número do cartão é codificado usando o método de criptografia RSA antes de ser enviado ao servidor e o banco usa a chave privada do seu servidor para decodificar o número que está no cartão e permite que a transação seja efetuada com sucesso. Na sala de aula será utilizado o RSA para garantir que as mensagens enviadas entre os alunos sejam seguras. Para isso os alunos irão realizar alguns cálculos para que se possa codificar e depois decodificar as mensagens. Essa atividade pode ser usada para discutir a importância da criptografia em ambientes profissionais. Será apresentado o processo de criptografia RSA com o auxílio dos teoremas apresentados nas aulas anteriores, assim como o conceito de chave pública na criptografia. Em seguida, novas atividades serão propostas (Tabela 16).
Objetivo específico: compreender o método de criptografar as informações através do RSA.

Tabela 16 – Problemas propostos para a turma-aula 8 - Lista 2.

Atividades:

1. Usando os primos 5 e 7, obtenha a chave de codificação (n, λ).
2. Obtenha uma chave de codificação (λ) segundo os critérios de criptografia RSA. (Converse com a turma e escolha uma chave padrão).
3. Considerando a tabela abaixo, construa a codificação da palavra "matematica":

A	10	N	23
B	11	O	24
C	12	P	25
D	13	Q	26
E	14	R	27
F	15	S	28
G	16	T	29
H	17	U	30
I	18	V	31
J	19	W	32
K	20	X	33
L	21	Y	34
M	22	Z	35

4. Agora envie para um colega da sala uma mensagem criptografada, utilizando a mesma tabela e chave pública para que ele possa decodificar a informação que você o enviou nas próximas aulas.

Fonte: Produção da própria autora.

A solução da Lista 2 considerando a codificação da mensagem "BOM DIA" está disponível no Apêndice B.

10ª aula
Tempo gasto estimado em duas aulas de 50 minutos cada.
Será apresentado o processo de decodificação de mensagens de acordo com os métodos de criptografia RSA. Para isso, tem-se como pré-requisito, o conceito de mostrar possíveis valores inteiros para uma equação de duas incógnitas. Em seguida, novas atividades serão propostas (Tabela 17).
Objetivo específico: compreender o método de decodificar as informações através do RSA.

Tabela 17 – Problemas propostos para a turma-aula 10 - Lista 3.

Atividades:

1. Encontre um par de solução (d, k) da equação $5d = 24k + 1$ em que o valor de d é o inverso de $5 \mod 24$.
2. De acordo com as aulas anteriores, você recebeu uma mensagem criptografada do seu colega. Agora é a hora de decodificar essa informação conforme a tabela ofertada na lista passada, os primos 5 e 7, e o d encontrado na questão 1.

Fonte: Produção da própria autora.

A solução da Lista 3 considerando a decodificação da mensagem "BOM DIA" está disponível no Apêndice C.

A sequência didática apresentada procurou propor aos estudantes um entendimento aprofundado dos conceitos de aritmética, de maneira que pudessem não apenas aprender o conteúdo, mas também aplicar o conhecimento desenvolvido, na área da computação, que é uma das ferramentas mais utilizadas pelos jovens. Ao longo das atividades, é esperado o desenvolvimento das habilidades cognitivas e o desenvolvimento na argumentação dos alunos, estimulando tanto o pensamento crítico quanto a capacidade de resolução de problemas.

6 Conclusão

Este trabalho começou a ser planejado durante as aulas de aritmética ainda no 2º semestre do curso do PROFMAT, com os ensinamentos do professor Dr. Valmecir Bayer. O objetivo é levar à sala de aula a sequência didática proposta no Capítulo 5 para estudantes como ferramenta do ensino da matemática, apresentada de maneira que a disciplina de matemática fosse relacionada ao tema da criptografia RSA, que mostrou sua aplicabilidade na área de conhecimento.

O primeiro assunto deste trabalho, expõe o desenvolvimento da criptografia ao longo dos séculos. No entanto, com o advento da era digital e a codificação de informações, tornou-se fundamental para a proteção de dados em praticamente todas as áreas da sociedade. Atualmente, o algoritmo criptográfico mais conhecido e utilizado é o RSA que garante a segurança de transações financeiras, comunicações privadas e sistemas computacionais, permitindo a troca segura de informações mesmo em redes públicas.

Ao longo da fundamentação teórica, observou-se que a criptografia RSA se baseia em conceitos matemáticos, principalmente na teoria dos números e na aritmética modular. Sendo necessários a demonstração de teoremas, proposições e corolários. São esses conhecimentos que garantem a eficácia do sistema.

Com a evolução da tecnologia, surgem novos problemas, como possíveis ataques baseados em algoritmos quânticos, que poderiam desqualificar a segurança do RSA ao resolver o problema da fatoração de números grandes em tempo executável. Sendo assim, a compreensão matemática do método não apenas justifica sua eficácia, mas também orienta pesquisas futuras na busca por novas formas de sistemas criptográficos, métodos mais resistentes a novas evoluções computacionais.

No decorrer do Capítulo 4, foi possível a organização do algoritmo RSA, desde a geração das chaves pública e privada até os processos de codificação e decodificação. A escolha adequada dos itens, especialmente dos primos p e q, do expoente de codificação λ e do cálculo da função Totiente de $\varphi(n)$. Além disso, a existência de d é essencial para a reversibilidade do processo de criptografia.

Durante o Capítulo 5, a metodologia proposta teve seus conteúdos embasados adequadamente para o Ensino Básico, envolvendo a parte histórica da evolução da criptografia, propriedades da teoria dos números e divisão Euclidiana, uso correto da calculadora como ferramenta pedagógica, atividades que estimularam a resolução de problemas desenvolvendo suas habilidades cognitivas. Essa sequência também promoveu a interdisciplinaridade da matemática com a história e a computação, trazendo assim, aplicações práticas da aritmética em seus aparelhos eletrônicos.

Referências

ANDRADE., E. G. de. Criptografia com curvas elípticas. *78f. Dissertação (Mestrado Profissional em Matemática - PROFMAT)-Universidade Federal do Pará Instituto de Ciências Exatas e Naturais*, 2016. Citado na página 24.

APOSTOL, T. M. *Introduction to Analytic Number Theory.* [S.l.]: Springer-Verlag., 1976. Citado na página 48.

BEZERRA D. DE J.; MALAGUTTIV, P. L. Aprendendo criptologia de forma divertida. *139f ed. Rio de Janeiro.*, 2010. Citado na página 65.

BRASIL. Ministério da Educação. Base nacional comum curricular. *Brasília: MEC.*, 2018. Citado 2 vezes nas páginas 14 e 73.

COSTA C.; FIGUEIREDO, L. M. Introdução à criptografia. *Disponível em: <https://canal.cecierj.edu.br/012016/a99b588e1edecbb6543d63cf51e20158.pdf>*, 2010. Citado 2 vezes nas páginas 13 e 17.

COUTINHO., S. C. Criptografia. *Rio de Janeiro, IMPA.*, 2015. Citado 2 vezes nas páginas 13 e 17.

DAVENPORT., H. *The Higher Arithmetic: An Introduction to the Theory of Numbers.* [S.l.]: Cambridge University., 2000. Citado na página 41.

FIARRESGA, V. M. C. Criptografia e matemática. *Universidade de Lisboa, Faculdade de Ciências, Departamento de Matemática*, 2010. Citado 3 vezes nas páginas 13, 15 e 18.

HARDY., G. H. *An Introduction to the Theory of Numbers.* [S.l.]: Oxford University., 2008. Citado na página 41.

HEFEZ, A. Aritmética. *1. ed. Rio de Janeiro: SBM. 338 p. (Coleção PROFMAT)*, 2014. Citado 9 vezes nas páginas 13, 25, 32, 40, 55, 57, 58, 60 e 70.

HOUAISS., A. Dicionário houaiss da língua portuguesa. *1. ed. Rio de Janeiro: Objetiva Instituto Antônio Houaiss de Lexicografia*, 1986. Citado na página 29.

LEVENIUS, L. G. Mersenne primes and the quest to find them. *30f. MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET.*, 2024. Citado na página 38.

LIMA, F. Éder Andrade de. Números primos e algumas curiosidades históricas: Da proposição infinita de euclides ao crivo de erastóstenes. *11f. Revista História da Matemática para Professores.*, 2024. Citado na página 37.

PAIXãO, J. S. d. Criptografia: história, atividades e divulgação científica. *Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. 174 p*, 2020. Citado na página 24.

SINGH, S. O livro dos códigos: A ciência do sigilo – do antigo egito à criptografia quântica. *4. ed. Rio de Janeiro: Record, 448p.*, 2004. Citado 6 vezes nas páginas 13, 15, 17, 18, 24 e 25.

TKOTZ, V. Criptografia - segredos embalados para viagem. 2005. Citado na página 22.

A Solução da lista 1

Tabela 18 – Solução dos problemas propostos para a turma-aula 5.

Atividades:

1. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de $4633 + 9349$ por 10?

   Solução: Pelo Teorema 5.1.1, apresentado durante a aula, pode-se concluir que o resto da divisão de $4633 + 9349$ por 10 é o mesmo do resto da divisão de $3 + 9$ por 10. $3 + 9 = 12 = 10 \cdot 1 + 2$. Portanto, o resto da divisão de $4633 + 9349$ por 10 é 2.

2. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de $9349 - 4633$ por 10?

   Solução: Pelo Teorema 5.1.1, apresentado durante a aula, pode-se concluir que o resto da divisão de $9349 + (-4633)$ por 10 é o mesmo do resto da divisão de $9 + (-3)$ por 10. $9 - 3 = 10 \cdot 0 + 6$. Portanto, o resto da divisão de $9349 + (-4633)$ por 10 é 6.

3. Sabendo que o resto da divisão de 4633 por 10 é 3, e o resto da divisão de 9349 por 10 é 9, então qual é o resto da divisão de 4633×9349 por 10?

   Solução: Pelo Teorema 5.1.2, apresentado durante a aula, pode-se concluir que o resto da divisão de 4633×9349 por 10 é o mesmo do resto da divisão de 3×9 por 10. $3 \times 9 = 27 = 10 \cdot 2 + 7$. Portanto, o resto da divisão de 4633×9349 por 10 é 7.

4. Ache o resto da divisão de 2^{100} por 11:

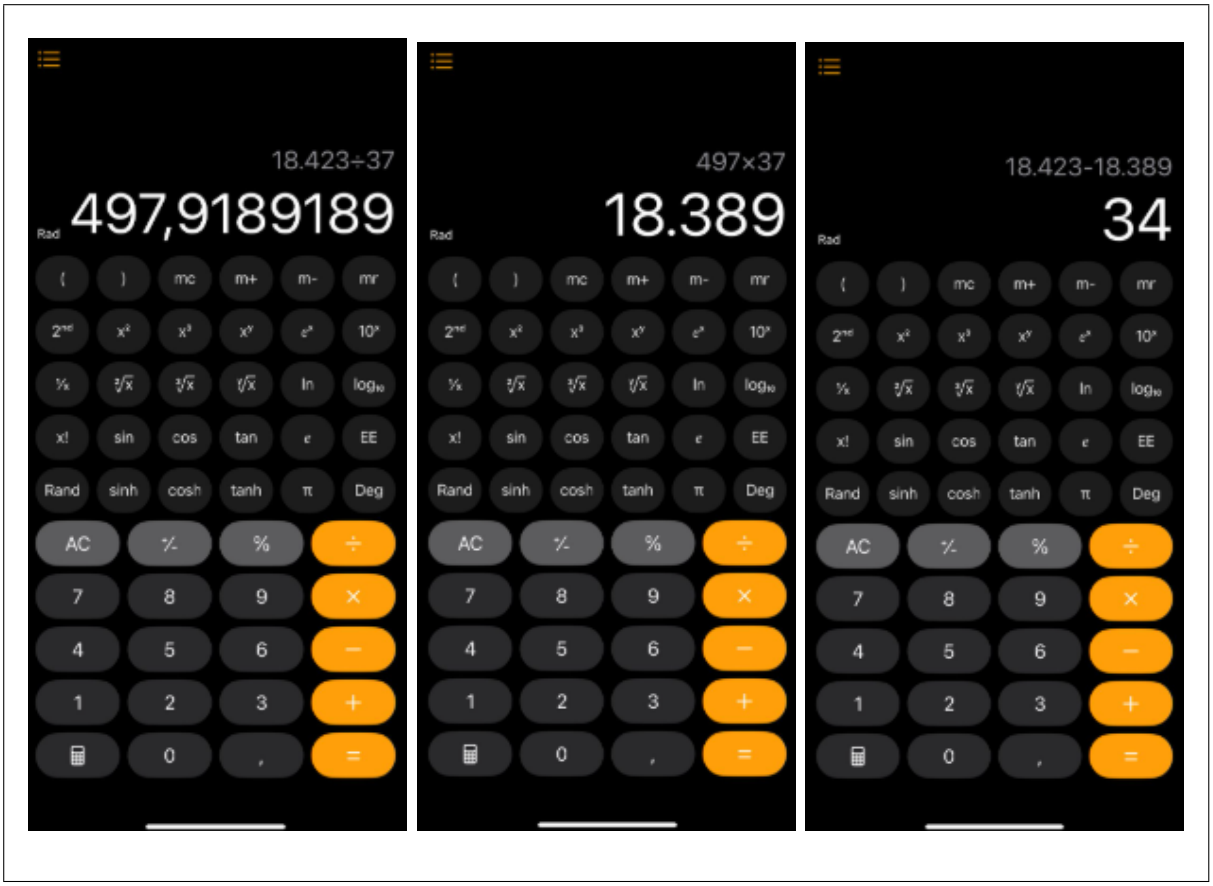
   Solução: Pelo Teorema 5.1.3, apresentado durante a aula e pelo conhecimento básico em propriedades de potência, tem-se que $2^5 = 32 = 11 \times 3 - 1$. Logo, o resto da divisão de 2^5 por 11 é -1. No entanto, 2^{100} pode ser escrito na forma $(2^5)^{20}$, então $(-1)^{20} = 1$ tem o mesmo resto que 2^{100}. Portanto, o resto da divisão 2^{100} por 11 é 1.

5. Ache o resto da divisão $12^{16} + 2^{100}$ por 11:

   Solução: Como já visto na solução da questão 4, que o resto da divisão de 2^{100} por 11 é 1 e pelo Teorema 5.1.3, apresentado durante a aula e pelo conhecimento básico em propriedades de potência, tem-se que $12 = 11 \times 1 + 1$. Logo, o resto da divisão de 12 por 11 é 1 e o resto da divisão de 12^{16} por 11 é $1^{16} = 1$. Portanto, o resto da divisão de $12^{16} + 2^{100}$ por 11 é $1 + 1 = 2$.

6. Com auxílio de uma calculadora, ache o resto da divisão de 18423 por 37

   Solução:



Fonte: Produção da própria autora.

B Solução da lista 2

Tabela 19 – Solução dos problemas propostos para a turma-aula 7.

Atividades:

1. Usando os primos 5 e 7, obtenha a chave de codificação (n, λ).

   Solução: Para obter a chave de codificação (n, λ) usando os primos $p = 5$ e $q = 7$, primeiro, será calculado n, que é o produto dos dois primos:

   $$n = p \times q = 5 \times 7 = 35$$

   Em seguida, será calculado $\varphi(n)$, que é a função Totiente de Euler para $n = p \times q$. Para dois números primos, $\varphi(n)$ é dada por:

   $$\varphi(n) = (p-1)(q-1)$$

   Substituindo $p = 5$ e $q = 7$ temos: $\varphi(n) = (5-1)(7-1) = 4 \times 6 = 24$

   Agora, escolhemos um valor para e, que deve ser um número inteiro tal que $1 < \lambda < \varphi(n)$ e λ seja coprimo com $\varphi(n)$, ou seja, $mdc(\lambda, \varphi(n)) = 1$.

   Testando alguns valores para λ: Quando $\lambda = 5$ verificou-se que $mdc(5, 24) = 1$.

   Portanto, $(n, \lambda) = (35, 5)$ é uma chave pública para a criptografia RSA.

2. Obtenha uma chave de codificação (λ) segundo os critérios de criptografia RSA. (Converse com a turma e escolha uma chave padrão).

   Solução: $\lambda = \{5; 7; 11; 13; ...\}$, por 5 ser o menor número possível, ele foi o escolhido.

3. Considerando a tabela abaixo, construa a codificação da palavra “matematica“:

A	10	N	23
B	11	O	24
C	12	P	25
D	13	Q	26
E	14	R	27
F	15	S	28
G	16	T	29
H	17	U	30
I	18	V	31
J	19	W	32
K	20	X	33
L	21	Y	34
M	22	Z	35

Solução: Usando a tabela fornecida:

M	A	T	E	M	A	T	I	C	A
22	10	29	14	22	10	29	18	12	10

Com auxílio de uma calculadora e considerando a como o resto da divisão, tem-se:

- $22^5 \div 35 = 5153632 \div 35 \Rightarrow a = 22$
- $10^5 \div 35 = 100000 \div 35 \Rightarrow a = 5$
- $29^5 \div 35 = 20511149 \div 35 \Rightarrow a = 29$
- $14^5 \div 35 = 537824 \div 35 \Rightarrow a = 14$
- $18^5 \div 35 = 1889568 \div 35 \Rightarrow a = 23$
- $12^5 \div 35 = 248832 \div 35 \Rightarrow a = 17$

A palavra **MATEMATICA** é criptografada como: $(22, 5, 29, 14, 22, 5, 29, 23, 17, 5)$

4. Agora envie para um colega da sala uma mensagem criptografada, utilizando a mesma tabela e chave pública para que ele possa decodificar a informação que você o enviou nas próximas aulas. **Solução:** Exemplo de mensagem codificada: $(16, 19, 22, 13, 23, 5)$

Fonte: Produção da própria autora.

C Solução da lista 3

Tabela 20 – Solução dos Problemas propostos para a turma-aula 9.

Atividades:

1. Encontre um par de solução (d, k) da equação $5d = 24k + 1$ em que o valor de d é o inverso de $5 \mod 24$.

   Solução: Dada a equação $5d = 24k + 1$ é necessário que o d seja isolado, em função de k. Sendo assim, a resolução deste problema fica $d = \frac{24k+1}{5}$, isso significa que é preciso encontrar um k que $24k + 1$ seja um múltiplo de 5.

   Testando os valores, tem-se:

   - Quando $k = 0$, $24 \cdot 0 + 1 = 1$ e $5 \nmid 1$
   - Quando $k = 1$, $24 \cdot 1 + 1 = 25$ e $\frac{25}{5} = 5$

   Portanto, o par de solução encontrado é o $(5, 1)$

2. De acordo com as aulas anteriores, você recebeu uma mensagem criptografada do seu colega, agora é a hora de decodificar essa informação conforme a tabela ofertada na lista passada, os primos 5 e 7, e o d encontrado na questão 1.

   Solução: Considere b o valor dos restos das divisões:

   - $16^5 \div 35 = 1048576 \div 35 \Rightarrow b = 11$
   - $19^5 \div 35 = 2476099 \div 35 \Rightarrow b = 24$
   - $22^5 \div 35 = 5153632 \div 35 \Rightarrow b = 22$
   - $13^5 \div 35 = 371293 \div 35 \Rightarrow b = 13$
   - $23^5 \div 35 = 6436343 \div 35 \Rightarrow b = 18$
   - $5^5 \div 35 = 3125 \div 35 \Rightarrow b = 10$

Usando a tabela fornecida na aula anterior:

11	24	22	13	18	10
B	O	M	D	I	A

Fonte: Produção da própria autora.